© THE QUEEN'S PRINTER FOR ONTARIO
2000

REPRODUCED WITH PERMISSION

L'IMPRIMEUR DE LA REINE POUR L'ONTARIO

REPRODUIT AVEC PERMISSION

micromedia
a division of IHS Canada

20 Victoria Street
Toronto, Ontario M5C 2N8
Tel.: (416) 362-5211
Toll Free: 1-800-387-2689
Fax: (416) 362-6161
Email: info@micromedia.on.ca

# A Consultation Paper:

# Proposed Ontario Privacy Act

**Prepared by**
**Ministry of Consumer and Commercial Relations**
**July 2000**

## Message from the Minister of Consumer and Commercial Relations

The Ministry of Consumer and Commercial Relations is today launching a public consultation to find the best way to protect the privacy of Ontarians when they deal with businesses and other non-government organizations.

Protecting personal privacy is a top priority for this government. We need to develop and maintain consumer confidence in the digital economy. This will help businesses seize the growing opportunities offered by today's global marketplace.

The federal government passed the *Personal Information Protection and Electronic Documents Act* (formerly Bill C-6) earlier this year. The Ontario government believes that there is a need to develop made-in-Ontario comprehensive protection of personal information, without imposing an excessive burden on businesses and not-for-profit organizations.

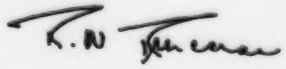
In addition to the general consultation on privacy, the Ministry of Health and Long-Term Care will be consulting on health information rules. More information on the health consultation will soon be available.

I am pleased to release *A Consultation Paper: Proposed Ontario Privacy Act* for review and comment and I encourage all interested parties to make submissions on the paper's proposals. Consultations will be held in locations across the province, to be announced later this month. Copies of the consultation paper are available on the ministry's Web site at http://www.ccr.gov.on.ca. Written comments and submissions should be sent, no later than September 15, 2000, to:

Ministry of Consumer and Commercial Relations
Privacy Consultation
250 Yonge St., 35th Floor
Toronto, Ontario M5B 2N5

Fax: 416-326-8885
E-mail: privacy@ccr.gov.on.ca

I look forward to hearing from you, and thank you for your interest in the proposals set out in Ontario's privacy consultation paper.



Robert W. Runciman, MPP
Leeds-Greenville
Minister of Consumer and Commercial Relations
July 20, 2000

100-06830/

## This Consultation Paper is About Privacy

The Ministry of Consumer and Commercial Relations is proposing to develop an Ontario Privacy Act which, if passed, would increase an individual's ability to control whether and how information about them is collected, used and disclosed. Clear privacy rules would also provide for the appropriate use and exchange of personal information by businesses and organizations.

The protection of personal information will foster consumer confidence in emerging technologies and build a supportive environment for business growth. By moving quickly to address growing public concerns about the use of personal information, Ontario will allow individuals and organizations to benefit from the opportunities offered by the digital economy.

We are extremely interested in receiving your comments on this proposal for an Ontario Privacy Act. In the paper, we ask a number of questions that focus on different approaches the legislation can take. The proposals in this consultation package are subject to the approval of the Legislature, and are intended for discussion purposes only.

We are asking for feedback from individuals, businesses and not-for-profit organizations. You can reply to us by fax, E-mail or regular mail -- please see the end of this paper for details. The paper is also available online at http://www.ccr.gov.on.ca. The last date for receiving comments will be September 15, 2000.

## Context

The use of information is at the heart of the efficiency and success of the digital economy and is a source of both tremendous economic potential and increased public concern.

*"Personal information" is information about an identifiable individual.*

As we move through our daily lives, an increasingly accessible and useable trail of information is left behind, often without our knowledge. That information can include: our address, telephone number, age, retail purchases, interests and financial status.

In fact, many of the benefits of the digital economy rely on the use of such personal information to serve the public in new ways that are convenient, useful and efficient. However, people are concerned about this flow of information for a number of reasons:

- The explosive growth of services, e-commerce sales and use of credit has increased the number and types of transactions leaving trails of personal information.
- Information can be collected from various sources to create personal profiles that may be used or sold without the knowledge or consent of the individual.
- Organizations such as non-profit groups or business partnerships trade or rent lists.

- Data-dependent fraud such as identity theft is growing.

> *"In today's global economy, jobs and investment can pick up and leave on very short notice. So, we have to stay competitive."*
>
> Blueprint, Mike Harris' Plan to Keep Ontario on the Right Track

In order to fully embrace new technologies and opportunities, the public needs to feel confident that personal information will be used appropriately. Organizations and marketplaces that gain the public's trust for their handling of personal information will have a strong advantage in a global economy.

Effective privacy legislation will provide a clear legal environment that inspires consumer and business confidence, and will support a more successful shift to electronic means of interacting and doing business. Through such legislation, Ontario will provide leadership in the new digital economy and foster public confidence.

Privacy is not a new concern. In 1980, the Organization for Economic Co-operation and Development (OECD) approved Guidelines on the Protection of Privacy and Transborder Data Flows of Personal Information. These guidelines were the first internationally developed standard for the treatment of personal information.

Since that time, several jurisdictions have implemented privacy laws to address public concerns about the use of personal information. In the United States, numerous bills related to personal privacy have been introduced in the federal and state legislatures in the past several months.

In Ontario's public sector, personal privacy is regulated under the *Freedom of Information and Protection of Privacy Act,* and the *Municipal Freedom of Information and Protection of Privacy Act.* These laws provide access to provincial and municipal government information and set rules for the collection, use and disclosure of personal information. The Ontario Information and Privacy Commissioner provides independent oversight of these Acts.

In Canada, the Canadian Standards Association Model Code for The Protection of Personal Information (CSA Standard) has been adopted as a National Standard. The CSA Standard is supported by a broad consensus of businesses, consumer organizations and provincial and federal governments. It sets out principles for privacy protection like those adopted by the Organization for Economic Cooperation and Development, the European Union and other jurisdictions.

> *We encourage you to review the CSA Standard. A summary of its principles can be found at Appendix A.*

The federal government's *Personal Information Protection and Electronic Documents Act*, formerly Bill C-6, which was passed in April, 2000, includes the CSA Standard as a schedule in the legislation. The federal legislation will initially apply to privacy in the federally regulated private sector (e.g., banking, telecommunications) and to cross-border commercial flows of information.

However, beginning in 2004, the federal legislation will apply to all commercial transactions in provinces without similar legislation in place. It would not apply to commercial transactions within Ontario if the province passes substantially similar legislation.

## Ontario's Goals in Developing Its Own Legislation

By acting now, Ontario can ensure that its rules for businesses and organizations are consistent with public expectations about the collection, use and disclosure of personal information. Given the global nature of e-business, Ontario must move quickly to position itself as a trusted marketplace in the new digital economy.

### Goal 1. Comprehensive and Seamless Privacy Protection

The proposed Ontario Privacy Act would provide comprehensive protection, including in areas not covered by the federal legislation, such as aspects of -- education, and provincially licensed professions. It would apply to all organizations and activities except government organizations covered by public sector legislation and organizations that are traditionally federally regulated (e.g., banks and cable companies).

> *"...comprehensive privacy legislation is necessary to preserve an individual's freedom of choice and to ensure that much-needed privacy protections are provided to all Ontarians."*
> 1999 Annual Report of the Ontario Information and Privacy Commissioner, Dr. Ann Cavoukian

An Ontario Privacy Act could also broaden privacy protection by applying to more than simply 'commercial' activities, as would be the case if Ontario does not act, and the federal legislation applies alone. For example, many non-profit organizations use personal information for non-commercial purposes, and employers use it internally in all organizations. Both Ontario and the federal government must act to provide comprehensive privacy protection.

### Goal 2. Flexibility for Unique Privacy Needs and Circumstances

People need timely and accurate information for good decision making in the health system. At the same time, health information is very personal and privacy must be protected. The proposed Ontario Privacy Act would include legislated rules setting out privacy requirements for health information. These rules would apply to personal information in the health sector, including private and public sector organizations. The Ministry of Health and Long-Term Care is conducting a consultation later this summer on health sector rules for the protection of personal information, and would be interested in receiving your feedback. For more information on the Protection of Health Information, please see Appendix B, or contact the Ministry of Health and Long-Term Care.

The proposed Ontario Privacy Act would also establish a rigorous process for the development of sector codes. A sector code is a set of rules that would tailor the proposed Act's requirements to a specific industry, type of information or way of using information. These codes would allow recognition of public needs within specific sectors, organizations or types of personal information.

Examples of where unique privacy rules may be appropriate are in the area of employee records and the use of personal information related to credit reporting, now covered in the *Consumer Reporting Act.*

**Goal 3. Efficient, Fair and Effective Enforcement**

Provincial legislation could provide workable rules for a wide variety of organizations, including smaller businesses that do not make extensive use of personal information or conduct business across the country. These rules would be clearly focused and reflect the substance of the CSA Standard without imposing an undue regulatory burden.

The result of such legislation would be to promote confidence in the Ontario marketplace and Ontario organizations, and to maximize opportunities for Ontario's success in the increasingly digital economy.

**Goal 4. Compatibility with Other Laws**

The proposed Ontario Privacy Act would be based on the CSA Standard, and would be similar in substance to the federal legislation. The proposed Act's application would be clearly defined to prevent overlap with existing provincial legislation including the *Freedom of Information and Protection of Privacy Act* and the *Municipal Freedom of Information and Protection of Privacy Act*. It would not override the privacy-related provisions of statutes such as the *Education Act* or the *Child and Family Services Act*.

## How Would an Ontario Law and the Federal Privacy Law Work Together?

The proposed Ontario Privacy Act would complement the substance of the federal law on the required conduct by organizations and the rights of individuals. Therefore, it is expected that an exemption would likely be granted by the federal government for matters governed under the proposed Ontario Act.

Most business organizations acting within Ontario would only have to be concerned with the Ontario law. Organizations that trade personal information outside of Ontario would still be affected by the federal legislation, as would traditionally federally regulated businesses. The similarity of the proposed Ontario Privacy Act and federal legislation would avoid occasional overlap becoming a source of conflict or confusion.

Ontario will work closely with the federal government and other jurisdictions to ensure harmonization of legislative requirements.

## Ontario's Proposed Approach Reflects the CSA Standard

Ontario fully endorses and supports the CSA Standard. In fact, Ontario is the only province to have participated in developing the CSA Model Code for the Protection of Personal Information.

The proposed Ontario Privacy Act would be based on the CSA Standard. However, although the CSA Standard is well suited to be applied as a voluntary code, not all of its elements may be well suited for legislation. Therefore, Ontario is considering each element of the CSA Standard and whether it would make an appropriate statutory requirement.

In some cases, the CSA Standard relies on recommendations for information management processes. Ontario's proposed legislation would focus on outcomes, and what is clearly required, rather than processes. In other words, although key provisions of the CSA Standard would be adopted, certain provisions would not be used in the proposed Ontario Privacy Act.

This drafting approach differs from the federal legislation's design, however the proposed Act would closely resemble the federal legislation on the key elements of the CSA Standard. The proposed Act would be drafted similarly to Quebec's privacy legislation, which has been in place since 1994 and is working well.

Later on in this paper, you'll be asked whether you agree with this approach to drafting the legislation.

## What Would Be Your Rights Under the Proposed Ontario Privacy Act?

Generally, the proposed Ontario Privacy Act would ensure individuals of three things:

1. You would have greater ability to control whether and how your personal information is collected, used and disclosed.

2. You would be able to see and, if necessary, correct your personal information.

3. You would be able to file a complaint if your personal information has been collected, used or disclosed in violation of the Act.

### Your Rights When Your Personal Information is Collected

Under the proposed Ontario Privacy Act, you would be asked to give your consent before your personal information is collected. An organization would have to explain what kind of personal information it is asking for and why. If the organization plans to disclose information about you to a third party, it would tell you the type of third party and explain why it is passing your information along. Then you would decide whether to give your consent.

Your consent would usually be "express" -- for example, by signing a paper or filling in an on-line form. The proposed Act would only allow "implied" consent in reasonable or obvious circumstances. For example, it would be reasonable for a newspaper to assume implied consent for using your home address if you call to buy a subscription for home delivery.

### Your Rights After Your Personal Information is Collected

The proposed Act would also let you withdraw your consent for the collection, use or disclosure of personal information. The organization would explain any implications of withdrawing your consent.

Under the proposed Act, you would not be able to withdraw your consent in order to break a contract. For example, you would not be able to stop a lender from using your personal

information in order to collect on a debt that you owe.

If your personal information has been provided to a third party, the organization would be required to help you identify the third party, so that you could withdraw consent for the third party's use of the information.

Under the proposed Act, you would not be denied a good, service or other transaction because you have refused to provide personal information for uses unrelated to the transaction.

**Who Can Provide Consent?**

An important question to consider is the age at which a minor can provide consent. In Ontario, the age of majority is 18. If the law does not clarify whether and when minors can consent to the collection and use of their personal information, there will be doubt about the validity of the consent of minors who provide personal information in the course of entering agreements, such as obtaining magazine subscriptions and club memberships.

The proposed Ontario Privacy Act could allow minors over a certain age, possibly 13, to give consent for the collection and use of their personal information in order to ensure that youth can engage in employment and commerce. In the codes of ethics of Canadian marketers, and in privacy legislation in the United States dealing with the minors and the Internet, the age of 13 has been adopted. Youth are also generally allowed to start working at the age of 14. If youth at this age could not consent to giving their personal information to prospective employers, it would affect their ability to complete a job application.

The proposed Act could set an age at which minors could give consent for the collection and use of their personal information. However, this ability would be limited to the particular interaction. Parental consent would be required for any unrelated use of the information, including subsequent disclosures. Parental consent would always be required for collecting information about minors under the set age.

The proposed Act would not change the age of consent for the use of personal information if it is addressed in another law.

Someone recognized by statute as having authority to act on behalf of an individual would also be able to provide or withdraw consent on that individual's behalf.

Here is the first of our 13 specific questions on the proposed general privacy law. These questions relate to proposals for a general Privacy Act, and do not apply to personal information in the health sector.
Please explain whether you support the issue described in the question, and provide us with any additional comments. You don't have to limit yourself to that issue - broader comment is welcome. A form is provided for your convenience.

**Question 1: Should the proposed Privacy Act include rules governing when minors can give consent?**

Yes, the Privacy Act should include rules for whether minors can give consent.

If yes, what age do you think is appropriate for minors being able to give consent?

No, the Privacy Act should not include rules for whether minors can give consent.

**Indirect Collection**

Often, personal information is provided by someone other than an individual themselves -- a third party. In other words, the individual does not provide the information directly, and so cannot give consent. For example, if you send flowers to someone, you give the florist the name and address of the person who will receive the flowers. Other examples of indirect collection without consent include: someone making a travel reservation for a friend, or purchasing a magazine subscription or book to be delivered as a gift.

Many of these activities are personal and family ones and involve an organization that would usually have to meet the proposed Act's obligations for obtaining consent to collect and use personal information.

It could be confusing if the proposed Act did not deal with this kind of indirect collection. People might be concerned about excessive use of indirect collection without consent. The proposed Act could describe limited situations where indirect collection without consent would be permitted.

For example, indirect collection would not be allowed in cases where that person might reasonably disapprove, or view this collection or use as undesirable.

**Question 2: Should the proposed Ontario Privacy Act include rules for the indirect collection of personal information without consent?**

Yes, the proposed Ontario Privacy Act would be clearer if it described limited indirect collection without consent for certain situations.

No, indirect collection should be addressed differently.

If no, how should the proposed Ontario Privacy Act address rules for indirect collection?

**Your Rights to Your Own Personal Information**

Under the proposed Ontario Privacy Act, you would be entitled to review your personal information, including information collected before the proposed Act came into force. You would also be entitled to be informed about how that information is used or disclosed to other organizations.

As in any law, some measure of reasonableness would apply. An organization would not be obliged to divulge trade secrets, violate solicitor-client privilege or put another person at risk in order to respond to your request for access to personal information.

Under the proposed Ontario Privacy Act, you would also be able to correct inaccurate personal information. If there is an unresolved disagreement about the accuracy of the information, you would have the right to have the information flagged as being disputed, such as an unresolved complaint between an organization and an individual about an outstanding debt. Privacy legislation is not appropriate or practical for resolving such disputes, but disputed information can be flagged.

## Your Organization Uses Personal Information - What Would be Your Organization's Obligations under the Proposed Act?

Under the proposed Ontario Privacy Act, your organization would have to respect an individual's control over the privacy of his or her personal information.

*Ontario firms and organizations will benefit if Ontario is perceived as a jurisdiction where privacy is protected.*

Collection of personal information would include transforming seemingly anonymous information into personal information through data analysis or combination.

### Would the Proposed Act Apply Regardless of the Kind of Organization?

Privacy is not a concern unique to the commercial world. Many non-commercial areas of activity involve personal information deserving privacy protection. For example, charities, universities, trade unions, professional associations, religious organizations and advocacy groups might collect personal information. This means the proposal for an Ontario Privacy Act is of interest to a broad range of organizations.

The proposed Ontario Privacy Act would apply to all businesses and not-for-profit organizations except government organizations covered by public sector legislation, and those organizations specifically subject to federal jurisdiction (such as banks and telecommunications). Certain activities would be exempted, such as the collection, use and disclosure of personal information for law enforcement purposes. These proposed exemptions are discussed later in the paper.

The proposed Ontario Privacy Act would not apply to personal, family and household uses of personal information, such as your mailing list for holiday greeting cards.

### How Would Your Organization Comply with the Proposed Act?

The proposed Ontario Privacy Act would involve five duties, all drawn from the CSA Standard. Your organization would normally have to:

1. Inform an individual what personal information you want to collect and why.
2. Obtain consent for the collection, use and disclosure of personal information.
3. Collect, use and disclose personal information according to the rules set out in the Act.

4. Provide access and correct errors to personal information when an individual requests it.
5. Keep personal information safe and dispose of it appropriately.

Under the proposed Act, your organization would only be permitted to collect, use or disclose personal information for purposes a person would consider appropriate in the circumstances. For example, it is not reasonable to collect racial or religious information for a transaction where human rights legislation prohibits you from using that information to make a decision.

The proposed Act would not require organizations to follow procedural steps, such as those specified in the CSA Standard's Accountability Principle, including implementing staff training and creating a privacy policy. These procedures are good business practices, but would not be required under the proposed law.

**How Would Your Organization Have to Collect Personal Information?**

Under the proposed Ontario Privacy Act your organization would normally have to inform a person why your organization is collecting personal information and obtain the person's consent.

Your organization's identified purpose would have to be meaningfully described. If your organization collects information to market products, it would not be enough to identify "marketing" -- instead, the type of products or the sort of retailer would need to be specified. For example, it would be acceptable to say that personal information would be used to market products your organization thinks are of interest to the individual, based on a survey the individual has filled out on consumer preferences.

Under the proposed Act, if it is not obvious, your organization would need to specify what information will be collected and how it will be collected (for example, by asking other organizations about the individual).

Your organization would also have to tell the person if it is going to give the information to a third party. The explanation should make it clear what kind of third party will receive the information and why.

These explanations would need to be given before, or at the time the information is collected.

**How Can Your Organization Obtain Consent?**

Under the proposed Act, your organization would ask for consent in a specific action or document, or through provisions in a contract or application form, where the person might be asked to agree to everything set out with one signature or action. Consent could cover a variety of future purposes and uses, as long as these have been clearly described beforehand.

Consent would be obtainable orally, in writing or electronically, as is reasonable in the circumstances.

The proposed Act would normally require your organization to obtain consent directly from the individual. However, it is proposed that another organization would be able to obtain consent for

your organization if it identified that it would disclose the information to an organization such as yours. In other words, if the individual was told his or her personal information might be given to an organization such as yours and gave consent, that organization could pass the information on to your organization. Similarly, your organization would be able to disclose information to another organization under similar circumstances (i.e., your organization obtained consent to do so).

Consent would be permitted through a clearly disclosed 'opt-out' option (i.e., by checking a box to prevent the use or disclosure of information about you) presented in a contract, application form or other process. An 'opt-out' approach could be implemented through a document to which the individual would otherwise have to signify agreement or through providing clear notice setting out a straightforward (and cost free) means of exercising the opt-out. It would not be acceptable for an organization to simply have a policy of permitting opting out if asked, without ensuring individuals are aware of their opportunity and have an easy means to use it.

The CSA Standard covers opt-out consent only in general terms. The proposed Ontario Privacy Act would clarify the use of opt-out consent, so as to avoid disputes.

**Question 3: Should "opt-out" consent be clearly permitted as an element of a contract, agreement or notice?**

Yes, the legislation should limit the use of the "opt-out" consent option as proposed.

No, the legislation should provide different rules for the use of "opt-out" consents (broader/narrower).

If no, should the legislation have more rules, or fewer rules for opting out?

**Can Your Organization Choose Not to Deal with Someone Who Withholds Consent?**

Under the proposed Ontario Privacy Act, your organization could choose not to deal with someone who withholds consent if that personal information is justifiably necessary for the transaction.

However, if the personal information does not relate to the transaction, your organization could not require the personal information in order to complete the transaction. The person would still have the right, for example, to buy your product or join your club without consenting to let your organization give his or her name and address to a third party for a secondary use. This means an individual would be able to withhold consent to unrelated uses of information in a contract, application form or other process.

The CSA Standard's provision on required consent only involves the supply of products and services, but the proposed Act would cover all transactions including, for example, landlord and tenant agreements and non-commercial transactions.

**When Would My Organization Be Able To Make Use of "Implied Consent"?**

Implied consent could save time for both individuals and organizations. The proposed Ontario Privacy Act would only allow implied consent in situations where expressly identifying your organization's purposes and obtaining consent are unnecessary. Implied consent would only apply to personal information directly related to a transaction, and the individual would still have to consent to any other use or disclosure of the information.

For example, it is reasonable to expect that an organization keeps financial and quality control records of transactions. These records are not normally disclosed outside the business and typically do not affect the individual. Your organization could rely on implied consent for such uses under the proposed Act.

*Your snow removal firm would be able to send a letter in the fall to its previous year's customers asking if they want to use your service again this year. However, you would have to respect customers' wishes if they said last year that they did not wish to receive other mail.*

It is proposed that where implied consent is appropriate, your organization would not have to expressly inform individuals of the purpose for collecting information, or expressly request consent. However, if someone asked, your organization would still have to fully explain how their information was used or disclosed.

Under the proposed Act, although the individual could still choose to withhold consent, in most cases involving implied consent it would be reasonable for your organization to decline to carry out the transaction. Implied consent usually involves information that is necessary for a transaction, so it would not be reasonable to go ahead without it. For example, a business cannot be denied the ability to keep internal audit records, or give an address to its delivery agents.

However, under the proposed Act implied consent would not be not sufficient when consent is needed for the disclosure of personal information to a third party. Implied consent would also not authorize collection of personal information from someone other than the individual or without the individual's knowledge. Also, implied consent would not extend to marketing additional or different products or services to a customer.

**Question 4: Should the legislation set out limited circumstances where implied consent would be appropriate, i.e., transactions that only involve internal and limited use of personal information?**

Yes, the legislation should allow implied consent in limited circumstances, such as internal business uses of information.

No, implied consent should be dealt with differently in the legislation.

If no, should the legislation define the use of implied consent more narrowly or more broadly? For instance, should it allow an organization to use the information to market unrelated products or services?

**Would My Organization Be Limited In Using Personal Information?**

Under the proposed Ontario Privacy Act, reasonable limits would apply. For example, if your organization changes its plans and wants to use personal information for different purposes than have already been explained to the individual, or wants to collect additional information beyond what was identified, your organization would have to obtain consent for the new collection, use or disclosure.

Your organization would be able to use outside assistance to do things such as data processing or to carry out marketing or fund-raising campaigns without express consent. The personal information could only be used if the individual has consented to such a use, or if it is authorized under the proposed Act. Both your organization and the outside firm would be held accountable for what happens to the information.

Under the proposed Ontario Privacy Act, your organization would have to keep records regarding disclosures of personal information to third parties. This means your organization would be able to provide access to the information to individuals on request, as required. This would not necessarily require a log of disclosures for each transaction, as long as your organization's arrangements are reasonably documented.

**What Are My Organization's Obligations to Retain or Dispose of Personal Information?**

Under the proposed Ontario Privacy Act, your organization would be able to keep personal information as long as needed to fulfil the purposes covered by consent, and to comply with any record retention required by law. Your organization would have to dispose of records, either by actually destroying the records or by rendering them anonymous. Your organization could meet this obligation by establishing a schedule for the disposal of information.

Your organization would also have to honour someone's withdrawal of consent for use of their personal information. The withdrawal of consent could not be retroactive and would be subject to reasonable limits.

It might be difficult sometimes to dispose of personal information because older paper records are not easily found or are not suitable for partial destruction. Personal information might also be contained in a record from which it cannot be deleted without harming the validity of the rest of the document, such as a contract or other legal document. Under the proposed Act, an organization would address these difficulties in its records management policies.

**What Safeguards Does My Organization Have to Take to Protect the Security of Personal Information?**

The proposed Ontario Privacy Act would require your organization to establish and apply security measures appropriate to the sensitivity of any personal information your organization holds. These measures would have to be reasonably sufficient to prevent unauthorized access, accidental or improper release, modification or use.

Under the proposed Act, your organization would have to explain your safeguards to anyone entitled to that information, such as prospective customers. The public description of safeguards would not have to be so specific that it would put your organization's security at risk. For example, you would not have to give details about Internet security that might inadvertently aid a hacker.

*If you use the Internet to take a credit card payment, you may need to identify what security safeguards are being used, such as encryption. The proposed Act would be drafted to ensure that it is technologically neutral.*

Although the proposed Act would not adopt the CSA Standard's Openness Principle, it would still be important for organizations' practices to be apparent and understandable to individuals. By requiring an organization to explain its safeguards, in addition to describing the sources of its personal information and the organizations to which it has disclosed personal information, the proposed Act would ensure that an organization's privacy practices are clear.

**Question 5: Should organizations be obliged to explain their safeguards?**

Yes, the proposed Act should clearly require that organizations explain their security safeguards.

No, the proposed Act does not need to require that organizations explain their security safeguards.

**What Happens When An Individual Requests Access to Personal Information?**

The proposed Act would require your organization to respond to requests for individual access to personal information, usually by granting that access. Your organization would also be required to allow a person to update, correct false information, and flag disputed information. Your organization would also need to be prepared to describe the sources of the personal information you have collected, and the organizations to which it has been disclosed.

The proposed Act would reflect the CSA Standard's Principle on Accuracy, but would make it clear that the legal requirement for accuracy creates a duty to record unresolved disagreements. Usually, a meaningful accuracy issue would arise as a request to correct information or withdraw consent. Although the law would address those issues, it should not become a forum to resolve disputes over the factual basis of information such as outstanding debts.

In cases where personal information has been used to deny a good or service to a person (for example, checking a credit application), your organization would be required to inform the person that they may review the information about them to ensure its accuracy.

When an individual asks to review information about themselves, the proposed Act would require your organization to provide the information within 30 days or inform the individual that the information will not be provided because of an exemption under the proposed Act.

There would be reasonable limits to your organization's obligation to provide access, similar to those cases where your organization would not have to destroy personal information (such as when it is impractical to locate it).

Under the proposed Act, your organization would be allowed to charge a cost-recovery fee for providing access to personal information. However if the information has been used to deny a benefit or increase a charge, individuals would be entitled to review the information free of charge.

The proposed Ontario Privacy Act would provide a means of avoiding abuse from nuisance requests (for example, if someone files a request every week for information that only changes every year).

**Question 6: Are the proposed rights of access and treatment of accuracy issues appropriate?**

Yes, the proposed Act's focus on access, correction of false information and flagging disputes is appropriate.

No, the accuracy of personal information should be subject to a statutory requirement.

**Would My Organization Be Able to Move Information Outside Ontario?**

The proposed Ontario Privacy Act would not prevent organizations from moving information within or outside Canada.

Within Canada, the federal *Personal Information Protection and Electronic Documents Act* would apply for commercial uses. Privacy laws of other provinces might also apply, where they exist.

Under the proposed Act, if your organization discloses personal information to someone outside Canada, particularly non-commercial information not covered by the federal legislation, your organization would be required to take reasonable steps to ensure the provisions of the proposed Ontario Privacy Act are respected. This could include adding provisions to contracts to make sure the personal information is only used for the purposes identified and for which the individual gave consent.

**Question 7: Should the proposed Act address moving information outside Ontario?**

Yes, the proposed Ontario Privacy Act should include rules for using contractual safeguards to ensure adequate privacy protection if information is sent to another jurisdiction.

No, the proposed Ontario Privacy Act should not address requirements for privacy protection outside its jurisdiction.

**What Would My Organization Have to Do Regarding Existing Personal Information Records?**

Under the proposed Ontario Privacy Act, your organization would have to respect the obligations for all personal information, including existing records.

The proposed transition period for a new Privacy Act would likely be one year. During this period your organization should review what personal information it holds and the uses for which it already has consent.

If your organization wants to continue using existing personal information or disclose it to others, it may have to contact individuals to provide the necessary information and obtain their consent.

**Question 8: Is the proposal for transition as an Act comes into force appropriate?**

Yes, the transition proposal is reasonable.

No, transition provisions should be different.

## Evaluating the Proposed Approach to Reflecting the CSA Standard

At this point, we want to know your comments about our approach so far.

The proposed Ontario Privacy Act attempts to balance meeting the strong public concern for privacy protection with the benefits of a clear regulatory regime that works well with the federal legislation.

Under the proposed Act, organizations would be held legally responsible for meeting the proposed privacy rules, but it would be up to organizations to implement steps necessary in order to comply with the law. Organizational matters such as staff training would not be subjects for investigation or complaint.

This approach differs from the federal legislation. However, both the federal legislation and the proposed Ontario Privacy Act are based on the CSA Standard, and the proposed Ontario Act would use its terminology and requirements as much as possible.

The rest of this paper addresses the need for flexibility and enforcement under the proposed Act. We want to combine clarity with a capacity for future flexibility and a role for effective enforcement.

**Question 9: Does the approach of the proposed Ontario Privacy Act strike an appropriate balance between meaningful privacy protection and clear, workable rules?**

Yes, the approach of the proposed Ontario Privacy Act makes sense.

Yes, the approach of the proposed Ontario Privacy Act makes sense overall but some modifications are desirable.

No, a different approach is recommended.

## Providing Flexibility for Unique Privacy Needs

The proposed Ontario Privacy Act must be technologically neutral and suitable for a broad range of organizations and types of personal information. However, although general rules would be appropriate for most organizations, specialized rules may be necessary for specific sectors. The proposed Act would also include two features to establish specialized privacy standards.

- A schedule to the proposed Act would set out privacy rules for the health sector.

- A process would also be set out for establishing and adapting privacy rules for specific sectors or types of personal information.

**Health Privacy Rules**

Good health care depends on the timely flow of information. Personal health information, however, should be shared only for a legitimate and sanctioned purpose. The Ministry of Health and Long-Term Care will be conducting a separate consultation on rules for acceptable collection, use or disclosure of personal information in the health sector.

Information about the proposed health sector rules and how you can participate in the consultation being conducted by the Ministry of Health and Long-Term Care is set out in Appendix B.

**Sector Codes to Respond to Unique Privacy Needs**

The proposed Ontario Privacy Act would allow the use of sector codes where necessary for the unique needs of a sector or type of personal information. A sector code is a set of rules that would tailor the proposed Act's requirements to a specific industry, type of information or way of using information.

Sector codes could clearly address issues and concerns specific to a particular sector or industry, with detail more appropriate than found in a general statute. Codes could change the application of some parts of the law to reflect the needs of a particular sector and develop information practices for particular issues. A sector code could be justified in a wide variety of areas, for example in particular economic sectors such as financial services or for a particular type of personal information such as employee records.

The proposed Act would set out a rigorous and transparent process for developing or changing a sector code. The process would require participation from representatives of the sector, the public interest and experts, as necessary (such as legal, technical, academic). It would require the final approval of the government.

Credit reporting is an example of an area that could be proposed as a sector code. There are already rules for the exchange of personal information used for credit reporting in the *Consumer Reporting Act*. It may make sense to address credit reporting as a sector under the proposed Ontario Privacy Act rather than under the current statute, so the laws do not overlap and are easier to oversee.

Experience in other jurisdictions suggests that there will not be many sector codes. A strong case would be required for any sector code to be developed. A sector code could not be simply a vehicle to advance the views or interests of one group at the expense of others. Any code would have to improve the overall privacy regime in Ontario.

**Question 10: Does the proposal for sector codes subject to a legislated process make sense?**

Yes, the proposal for sector codes subject to a legislated process makes sense.

No, the proposed Ontario Privacy Act should not permit the development of sector codes as suggested. If no, what process should the law provide for their development or approval?

No, the proposed Ontario Privacy Act should not permit the development of sector codes.

## What Exemptions and Exceptions Would Apply?

It is proposed that, in certain situations, it would not be necessary to require an individual's consent to collecting, using or disclosing personal information. Exemptions from the consent and/or access requirements in the proposed Ontario Privacy Act would be used to help ensure the safety, health or security of our communities, or to balance the protection of personal information with other essential rights, such as freedom of speech.

The proposed exemptions address the same issues covered by federal privacy legislation in order to avoid confusion between the two laws.

**When Can Information Be Collected, Used or Disclosed without the Individual's Consent?**

**Law Enforcement:** The proposed Act would not prevent individuals or organizations from cooperating with law enforcement. It would also allow a person or an organization to disclose personal information to law enforcement agencies if there are reasonable grounds to suspect an offence.

**Journalism, Art and Literature:** The proposed exemption would not affect other legal remedies such as defamation or libel. Journalistic and similar organizations would not be completely exempt. A newspaper would still need consent to sell its subscriber list.

**The Welfare of the Individual:** Consent would not be required if using personal information is clearly in the individual's presumed interest and the individual's express wishes cannot be determined.

**Private Enforcement of Contractual Rights:** The proposed exemption would not remove existing protections under other legislation, such as consumer protection for debt enforcement.

**Public Domain Information:** The proposed exemption would apply to information in the public domain (such as the Corporations Registry or court records).

**Statutory Authorization:** The proposed exemption would apply where another law, federal or provincial, provides authority for the collection, use or disclosure of personal information.

**Solicitor-Client Privilege:** The proposed exemption would respect solicitor-client privilege so that individuals can exercise the various legal rights and actions available to them.

**Historical Purposes:** The proposed exemption would allow for the conservation of records of historic or archival importance.

**When Would Individuals Not Be Able to Access Their Personal Information?**

Under the proposed Act, individuals may not be able to access all of their personal information in the following situations;

**Law Enforcement:** An organization would not have to place an investigation at risk by revealing that it has provided information to a law enforcement agency.

**Solicitor-Client Privilege:** Any exemption would apply only to information subject to privilege.

**Conflicting Personal Interests:** An individual would not have a right to access personal information if another person's welfare is involved.

**Trade Secrets:** An exemption would apply if providing access to personal information would reveal trade secrets. To whom a company has disclosed personal information, and for what purpose, would not be considered a trade secret.

Exemptions to access to personal information would usually require that as much information be disclosed as possible, so that only sensitive information would be withheld.

**What Exceptions Would There Be Under the Proposed Act?**

**Research:** Under the proposed Act, a research exception would only be authorized on request where the purpose of the research requires personal information and obtaining individual consent is not practical. For example, under the proposed Act privacy rights would continue for a period of 30 years after an individual's death, consistent with Ontario's *Freedom of Information and Protection of Privacy Act*. A research exception might be possible if it is difficult to find someone able to consent for access to such records. The proposed Act would require the public interest in permitting research be weighed against individual interest in personal privacy.

**Trade Secrets:** Under the proposed Act, a claim could be made that a threat to the life, health or security of an individual should override the trade secret exemption to access.

**Question 11: Are the exemptions and exceptions to the proposed Ontario Privacy Act reasonable?**

Yes, the exemptions and exceptions to the proposed Ontario Privacy Act are reasonable.

No, some areas should not be exempted or excepted from the proposed Ontario Privacy Act. If no, which areas?

Are there other exemptions or exceptions which should be included in the proposed Ontario

Privacy Act? If so, please describe them.

## How Would The Proposed Ontario Privacy Act Be Enforced?

Similar to the federal legislation, the proposed Ontario Privacy Act would make a specific body responsible for compliance with the legislation.

Ontario's goal is to have a single body responsible for compliance with all provincial privacy legislation. We are seeking feedback on what enforcement provisions are appropriate for privacy rules which apply to businesses and other organizations.

The existing public sector legislation, including the *Freedom of Information and Protection of Privacy Act* and the *Municipal Freedom of Information and Protection of Privacy Act*, establishes the Ontario Information and Privacy Commissioner as its independent oversight body. This paper is not seeking comments on the public sector legislation, or its oversight mechanisms.

The Commissioner's views are being sought on the proposals in this paper and, in particular, on appropriate enforcement powers.

You will be asked at the end of this section for your opinion on each of the enforcement powers or issues proposed. Comments on the proposals will help determine the role of the body to be made responsible for compliance with Ontario's privacy laws.

### Successful Regulatory Law

The proposed Ontario Privacy Act aims to provide clear, meaningful rules and avoid red tape or undue regulatory burdens.

Fair information practices are good business practices. Many leading corporations are adopting new principles for the management of personal information. We anticipate most organizations would see the economic benefits of quickly adopting the rules set out in the proposed Ontario Privacy Act.

If we look at the experience of the business community, with compliance with legislation for marketplace standards, we can see that effective enforcement complements the legislation. All retail businesses are subject to laws such as the *Business Practices Act* and the *Consumer Protection Act*, yet most businesses, because they are concerned about customer service, do not need to worry about investigation, prosecution or even civil suits under these acts.

Only a minority of organizations seriously try to profit from breaking the law. Strong enforcement action is aimed at this minority. Most often, the business community supports this enforcement action and sometimes requests it. It views persistent non-compliance as an attempt to gain an unfair competitive advantage and a threat to the reputation of honest members of the same sector.

Without effective enforcement, the Ministry of Consumer and Commercial Relations believes that both the public and organizations will eventually view a privacy law as flawed.

**What Enforcement Actions Would the Proposed Act Authorize?**

The proposed Act would provide a variety of options for enforcement. Available actions would include:

- the ability to mediate disputes or recommend mediation by outside parties;
- the ability to order organizations to change information practices to comply with the law (i.e., compliance orders);
- the ability to publicize findings; and
- offences for which charges could be laid and prosecuted.

As with other areas of regulation, it would not be necessary to use all the powers of the proposed Act to resolve most complaints and disputes. In fact, based on the experience of the Quebec Privacy Commission, mediation and consultation are expected to resolve most complaints and disputes.

Under the proposed Act, if someone thinks an organization has not collected, used or disclosed his or her personal information according to the law, the person should first contact the organization directly to try to resolve the problem. If the parties cannot resolve the situation, mediation could then be authorized.

The proposed Act would provide for action to be taken on individual complaints or other reasonable grounds, such as: information from a concerned employee, or a competitor who feels unfair advantage is being gained by a privacy violation.

Similar to federal legislation, the proposed Act would provide "whistleblower protection" to protect employees, who report privacy infractions, from reprisal.

The proposed Act would provide investigation powers similar to those in other statutes governing business activity and consumer protection. Those powers would include investigation powers for making inquiries when there are reasonable and probable grounds to believe there has been a violation. Search warrants would be required for any extraordinary collection of evidence related to a potential offence or for entry into a personal residence to find evidence of a potential offence.

Under the proposed Act, obstructing an investigation or destroying evidence would be prohibited.

**Compliance Orders and Assurances**

Under the proposed Act, compliance orders could be used to ensure organizations take corrective action without assigning penalties or blame. To issue an order, there would need to be reasonable and probable grounds to believe a violation has taken place. For example, if information was used inappropriately or a person was denied access to his or her own personal information, an order

might require an organization to do one or more of the following:

- provide the person with the personal information;
- stop or change a particular prohibited information practice (such as stop releasing information to a third party);
- implement procedures to ensure compliance with the proposed Act (such as documentation or security measures).

In some cases, an organization could also make an assurance of voluntary compliance. An assurance would be a legally binding promise to voluntarily undertake corrective action and would be made before a compliance order is issued. An assurance would have the same legal force as an order and be equally public. Violation of either a compliance order or an assurance would be an offence.

Under the proposed Act, offering to make an assurance would not guarantee its acceptance, and would not mean an enforcement agency would not issue a compliance order or pursue stronger remedies.

By offering or making an assurance, an organization would not be admitting any wrongdoing. However, the assurance might commit an organization to an action it might not otherwise have undertaken (such as publishing special notices to customers or public education).

**Appeals**

The ability to appeal decisions is a fundamental principle of many regulatory regimes. Where an individual or organization is subject to administrative decisions that have a material impact, such as a compliance order, the individual or organization often has the right to appeal the decision.

Under the proposed Ontario Privacy Act, an appeal process could be created. An appeal could be heard by an independent body such as the courts or a specialized tribunal that is independent of the decision-maker whose judgement is being appealed. Such appeals are provided in many statutes governing marketplace standards (such as the *Business Practices Act*).

A specialized tribunal can often offer a better understanding of the issues, and a more timely and cost-effective disposition of appeals than the courts. A quick method of resolving questions can be useful to organizations and individuals.

If a tribunal was created, appeals to the courts would continue to be permitted on questions of law.

**Question 12: Should the proposed Ontario Privacy Act provide for appeals without the necessity of going to court?**

Yes, an administrative process should be available for appeals of enforcement actions.

No, the only appeal mechanism should be the courts.

**What Would Be Considered An Offence Under the Proposed Act?**

Most enforcement problems would likely be resolved through mediation, compliance orders and assurances. Prosecution for an offence would be used for deliberate violations of the proposed Act.

Potential offences under the proposed Act could include contravening the key requirements of the legislation:

- collecting, using or disclosing personal information in conflict with the proposed Act;
- refusing to provide individuals with access to their personal information;
- obtaining someone else's personal information under false pretences;
- obstructing investigations including destroying or disposing of personal information or lying to investigators;
- violating a compliance order or assurance of voluntary compliance.

Fines authorized by the proposed Act would be consistent with other administrative statutes. Most administrative statutes currently impose potential fines of up to $50,000 for individuals and up to $500,000 for corporations or other organizations.

**Is a Person Limited to Relying on Enforcement of the Proposed Act?**

Under the proposed Ontario Privacy Act, individuals would be able to sue in civil courts where damages arise as a result of a violation of their rights under the proposed Act.

*The ability to pursue a private remedy is a feature of the common law. Marketplace standards legislation does not typically remove rights of civil action.*

To ensure the ability to efficiently enforce the proposed Act and resolve privacy disputes, people engaged in the enforcement of the proposed Act could not be called as witnesses in civil actions.

**Question 13: Do you agree with the proposal that the proposed Act provide for the following:**

| | |
|---|---|
| Mediation: | Yes___ No ____ |
| Investigation Authority: | Yes___ No ____ |
| Compliance Orders: | Yes___ No ____ |
| Assurances of Voluntary Compliance: | Yes___ No ____ |
| Support for Civil Remedies: | Yes___ No ____ |
| Offences: | Yes___ No ____ |

If you believe there should be other investigation or enforcement powers, please suggest them.

## Conclusion

**This proposal does not represent Ontario's final views on how to best frame an Ontario Privacy Act.**

**Your comments and views are an essential part of deciding the shape of privacy protection in Ontario. We welcome all your input on the specific questions we have asked, and on any other aspect of the proposed legislation. Please indicate whether you are commenting as an individual or on behalf of an organization.**

**Please submit your comments to any one of the following:**

Ministry of Consumer and Commercial Relations
Privacy Consultation
250 Yonge Street, 35th Floor
Toronto, Ontario
M5B 2N5

**Fax: (416) 326-8885**

**privacy@ccr.gov.on.ca**

**The Ministry of Consumer and Commercial Relations has been directed to consult with the public regarding how best to frame Ontario privacy legislation. Any personal information you provide is subject to the *Freedom of Information and Protection of Privacy Act*. The information will be used to assist us in conducting and evaluating the results of the consultation, which may involve disclosing your comments to other participants, institutions and interested parties during and after the consultation. Your name will not be disclosed without your consent.**

**If you have any questions about the collection, use or disclosure of this information, please contact:**

**The Freedom of Information and Privacy Coordinator**
**Ministry of Consumer and Commercial Relations**
**(416) 326-8470**

## APPENDIX A:
## CSA Model Code for the Protection of Personal Information, Principles in Summary

With the permission of CSA International, material is reproduced from CSA Standard CAN/CSA-Q830-96, Model Code for the Protection of Personal Information, which is copyrighted by CSA International, 178 Rexdale Boulevard, Etobicoke, Ontario, M9W 1R3. While use of this material has been authorized, CSA International shall not be responsible for the manner in which information is presented, nor for any interpretation thereof.

If you would like further information on the CSA Model Code for the Protection of Personal Information, or to purchase a copy of the publication, please contact the CSA International at (416) 747-4044, or 1-800-463-6727, or visit their Web site at http://www.csa-international.org

Ten interrelated principles form the basis of the CSA Model Code for the Protection of Personal Information. Each principle must be read in conjunction with the accompanying commentary.

**1. Accountability**

An organization is responsible for personal information under its control and shall designate an individual or individuals who are accountable for the organization's compliance with the following principles.

**2. Identifying Purposes**

The purposes for which personal information is collected shall be identified by the organization at or before the time information is collected.

**3. Consent**

The knowledge and consent of the individual are required for the collection, use or disclosure of personal information, expect where inappropriate.

**4. Limiting Collection**

The collection of personal information shall be limited to that which is necessary for the purposes identified by the organization. Information shall be collected by fair and lawful means.

**5. Limiting Use, Disclosure and Retention**

Personal information shall not be used or disclosed for purposes other than those for which it was collected, except with consent of the individual or as required by law. Personal information shall be retained only as long as necessary for the fulfilment of those purposes.

**6. Accuracy**

Personal information shall be as accurate, complete, and up-to-date as is necessary for the purposes for which it is to be used.

**7. Safeguards**

Personal information shall be protected by security safeguards appropriate to the sensitivity of the information.

**8. Openness**

An organization shall make readily available to individuals specific information about its policies and practices relating to the management of personal information.

**9. Individual Access**

Upon request, an individual shall be informed of the existence, use, and disclosure of his or her personal information and shall be given access to that information. An individual shall be able to challenge the accuracy and completeness of the information and have it amended as appropriate.

**10. Challenging Compliance**

An individual shall be able to address a challenge concerning compliance with the above principles to the designated individual or individuals accountable for the organization's compliance.

## APPENDIX B:
## Health Sector – Rules for Protection of Personal Health Information

Timely and accurate information is vital to support good decision-making in the health system – whether for making a diagnosis when urgent care is needed or for planning how health services should be organized and delivered, or for searching for new and improved ways of treating illness.

However, health information is also very personal, and people's privacy must be protected. There must be limits on how and when health information is shared.

Legislated rules for health information in the health sector must strike the right balance between protecting privacy and making sure that health information can be used carefully and appropriately to improve care and the management of the health system.

It is also important that the same rules apply to all parts of the health sector, from physicians' offices to laboratories to emergency rooms. Clear health privacy rules will support government reforms such as Primary Care Reform and Smart Systems for Health, and other initiatives to improve the integration of health services. Without common rules, such initiatives will be seriously impeded in achieving better coordination of health services and soundly based planning for improvements to the health system.

The Ministry of Health and Long-Term Care is in the late stages of developing legislated rules to protect personal health information.

The Ministry has carried out two extensive rounds of consultation. In June 1996, a consultation paper, "A Legal Framework for Health Information," was widely distributed for comment, and regional roundtable meetings were led by then Parliamentary Assistant to the Minister Helen Johns. In November 1997, a draft act for discussion purposes called the *Personal Health Information Protection Act, 1997*, was widely distributed for comment, and regional roundtable meetings were led by then Parliamentary Assistant to the Minister Tim Hudak. The purpose of this last round of consultation is to inform stakeholders about progress of the legislation since the previous consultations as well as seek further comments.

It is anticipated that, once an Ontario Privacy Act is in place, the health sector rules for health information will be incorporated into the statute as a code in the form of a separate schedule. The Ministry of Health and Long-Term Care will be conducting a consultation on draft rules for health privacy in the near future.

Please contact the Ministry of Health and Long-Term Care about receiving a copy of the consultation document, once released at (416) 327-4327, TTY 1-800-387-5559 or toll free 1-800-268-1153.

ISBN 0-7778-9991-4

07/2000

© Queen's Park Printer for Ontario, 2000

Ontario

# Document pour consultation :

# Proposition de loi ontarienne sur la protection des renseignements personnels

**préparé par**
**le ministère de la Consommation et du Commerce**
**juillet 2000**

## Message du ministre de la Consommation et du Commerce

Le ministère de la Consommation et du Commerce amorce aujourd'hui des consultations publiques dans le but de trouver la meilleure façon d'assurer la protection des renseignements personnels des Ontariens lorsque ceux-ci traitent avec des entreprises et des organismes non gouvernementaux.

La protection des renseignements personnels est la priorité absolue de ce gouvernement. Nous devons renforcer et soutenir la confiance des consommateurs dans l'économie numérique, ce qui permettra aux entreprises de tirer parti des nouvelles perspectives qu'offre le marché mondial.

Plus tôt cette année, le gouvernement fédéral a adopté la *Loi sur la protection des renseignements personnels et les documents électroniques* (projet de loi C-6). Le gouvernement de l'Ontario est d'avis qu'il est nécessaire que cette province se dote de mesures visant à assurer la protection intégrale des renseignements personnels, sans pour autant imposer de fardeau administratif aux entreprises et aux organisations à but non lucratif.

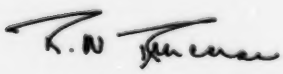
Outre les consultations générales sur la protection des renseignements personnels, le ministère de la Santé et des Soins de longue durée tiendra des consultations au sujet des règles visant la protection des renseignements médicaux personnels. De plus amples renseignements à ce sujet seront diffusés sous peu.

Je suis heureux de rendre public le document de consultation intitulé *Proposition de loi ontarienne sur la protection des renseignements personnels* aux fins d'examen et de commentaires. J'invite toutes les parties intéressées à présenter leurs observations sur les propositions énoncées. Des consultations, qui auront lieu dans diverses localités de la province, seront annoncées plus tard au cours du mois. On peut obtenir un exemplaire du document de consultation au site Web du Ministère à http://www.ccr.gov.on.ca. Les mémoires et les commentaires doivent nous être adressés par écrit, au plus tard le 15 septembre 2000, comme suit :

Ministère de la Consommation et du Commerce
Consultation sur la protection des renseignements personnels
250, rue Yonge, 35e étage
Toronto (Ontario) M5B 2N5

Télécopieur : (416) 326-8885
Courriel : privacy@ccr.gov.on.ca

J'attends avec plaisir vos observations et je vous remercie de l'intérêt que vous manifestez à l'égard des propositions énoncées dans le document de consultation.



Robert W. Runciman, député provincial
Leeds-Grenville
Ministre de la Consommation et du Commerce
le 20 juillet 2000

## Ce document pour consultation porte sur la protection des renseignements personnels

Le ministère de la Consommation et du Commerce propose d'élaborer une loi ontarienne sur la protection des renseignements personnels qui, si elle est adoptée, donnerait aux particuliers une capacité accrue de contrôle sur la façon dont les données les concernant sont recueillies, utilisées et divulguées; des règles claires de protection des renseignements personnels permettraient aussi d'assurer une utilisation et des échanges appropriés de données personnelles par et entre monde des affaires et organisations.

Cette politique de protection des données personnelles entraînera une plus grande confiance des consommateurs envers les nouvelles technologies et un appui plus solide en faveur de la croissance des affaires. En répondant ainsi rapidement aux préoccupations croissantes du public à propos de l'utilisation des données personnelles, l'Ontario permettra aux particuliers et aux organisations de mieux profiter des occasions qu'offre l'économie numérique.

Nous sommes très anxieux de recevoir vos commentaires sur cette proposition de loi ontarienne sur la protection des renseignements personnels. Dans ce document, nous posons un certain nombre de questions qui sont axées sur les diverses approches qu'une telle législation pourrait adopter. Les propositions soumises à cette consultation doivent être approuvées par le parlement et elles ont pour seul objectif d'alimenter le débat.

Dans notre quête de commentaires, nous nous adressons aux particuliers, au monde des affaires et aux organisations sans but lucratif. Vous pouvez nous répondre par télécopieur, courrier électronique ou courrier régulier -- vous trouverez tous les détails à la fin de ce document; ce dernier est aussi disponible « en ligne » http://www.ccr.gov.on.ca. Nous accepterons les commentaires jusqu'au 15 septembre 2000.

## Contexte

L'utilisation de données personnelles est au coeur même de l'efficacité et du succès de l'économie numérique; elle est à la fois une source de développement économique extraordinaire et de préoccupation croissante au sein du public.

*« Les données personnelles » sont des renseignements sur une personne identifiable.*

Tandis que nous vaquons à nos occupations quotidiennes, nous laissons derrière nous une piste faite de données personnelles qui peuvent être relevées et utilisées de plus en plus facilement, souvent sans même que nous nous en rendions compte. Ces données pourraient être notre adresse, notre numéro de téléphone, notre âge, nos achats, nos goûts ou notre situation financière.

De fait, de nombreux avantages de l'économie numérique reposent précisément sur l'utilisation de telles données qui permet de servir le public de façons à la fois nouvelles, pratiques, utiles et efficaces. Pourtant, ce flot de renseignements inquiète les gens pour un certain nombre de raisons :

- La croissance explosive des services, des ventes et du crédit qu'entraîne le cybercommerce a augmenté considérablement le nombre et les types de transactions qui laissent derrière elles des pistes de données personnelles.

- Ces données peuvent être obtenues de sources variées et permettent de créer des listes de fiches personnelles qui peuvent ensuite être utilisées ou vendues sans que les personnes concernées le sachent et aient donné leur accord.

- Des organisations, comme les groupes sans but lucratif ou les partenariats d'affaires, échangent ou louent de telles listes.

- Les fraudes qui reposent sur l'utilisation de données personnelles, comme le vol et l'utilisation de l'identité d'autres personnes, augmentent rapidement.

> *« Dans le contexte de globalisation actuel, emplois et investissements peuvent apparaître et disparaître sans grand préavis, d'où l'importance de maintenir notre compétitivité ».*
>
> Plan d'action : le programme de Mike Harris pour maintenir l'Ontario sur la bonne voie.

Pour pouvoir se rallier sans réserve aux nouvelles technologies et saisir les occasions qu'elles offrent, le public doit être convaincu que les données personnelles seront utilisées de façon appropriée. Les organisations et entreprises privées capables de gagner la confiance du public par leur façon d'utiliser les données personnelles, disposeront d'un atout puissant dans une économie globalisée.

Une loi efficace sur la protection des renseignements personnels créera un environnement juridique clair susceptible d'inspirer la confiance des consommateurs et des milieux d'affaires et appuiera avec plus de succès la conversion à des moyens électroniques d'interaction et d'affaires. Une telle législation permettra à l'Ontario de jouer un rôle de leader dans le passage à cette nouvelle économie numérique et aussi de gagner la confiance du public.

La protection des renseignements personnels n'est pas une nouvelle préoccupation. Déjà en 1980, l'Organisation de coopération et de développement économiques (OCDE) approuvait des lignes directrices sur la protection des renseignements personnels et sur le flux transfrontière des données personnelles. Ces lignes directrices étaient donc les premières normes développées au niveau international pour le traitement des données personnelles.

Dès lors, plusieurs pouvoirs législatifs ont mis en place des lois sur la protection des renseignements personnels afin de répondre aux préoccupations du public concernant l'utilisation des données personnelles. Aux États-Unis, de nombreux projets de lois touchant à la vie privée ont été déposés tant au niveau fédéral qu'au niveau des états, au cours des quelques mois passés.

Dans la fonction publique ontarienne, la protection des renseignements personnels est régie par la *Loi sur l'accès à l'information et la protection de la vie privée* et par la *Loi sur l'accès à l'information municipale et la protection de la vie privée*. Ces lois donnent accès aux renseignements des gouvernements provincial et municipaux et établissent les règles de cueillette, d'utilisation et de divulgation des données personnelles. La Commissaire à l'information et à la protection des renseignements personnels de l'Ontario assure une surveillance indépendante de ces lois.

*Nous vous encourageons à étudier la norme CSA. Vous en trouverez un résumé à l'annexe A.*

Au Canada, on a adopté comme norme nationale, le Code type sur la protection des données personnelles de l'Association canadienne de normalisation (norme CSA). La norme CSA est appuyée par un large consensus entre le monde des affaires, les organisations de consommateurs ainsi que les gouvernements fédéral et provinciaux. Elle établit des principes pour la protection des renseignements personnels, similaires à ceux qui ont été adoptés par l'Organisation de coopération et de développement économiques, l'Union européenne et d'autres pouvoirs législatifs.

La *Loi sur la protection des renseignements personnels et les documents électroniques* inclut la norme CSA comme annexe à la législation; c'est une loi du gouvernement fédéral, anciennement projet de loi C-6, qui a été adoptée en avril 2000. Au début, cette législation fédérale s'appliquera à la protection des renseignements personnels dans les segments du secteur privé sous juridiction fédérale (les banques, les télécommunications, etc) ainsi que dans les flux commerciaux transfrontières de données.

Dès le début de 2004, cependant, cette législation fédérale s'appliquera à toutes les transactions commerciales dans les provinces qui ne disposeront pas d'une législation similaire. Elle ne s'appliquera pas aux transactions commerciales dans la province de l'Ontario dans la mesure où cette dernière se sera dotée d'une législation similaire.

## Objectifs de l'Ontario dans le développement de sa propre législation

En agissant maintenant, l'Ontario s'assure que ses règles pour le monde des affaires et les organisations répondent aux préoccupations du public concernant la cueillette, l'utilisation et la divulgation de données personnelles. Étant donnée la nature globale des cyber-affaires, l'Ontario doit se positionner rapidement comme une région digne de confiance pour la nouvelle économie numérique.

### Objectif 1. Une protection des renseignements personnels complète et continue

La loi sur la protection des renseignements personnels, proposée par l'Ontario, fournirait une protection complète, y compris dans des domaines qui ne sont pas couverts par la législation fédérale, tels certains aspects de l'éducation et des professions qui sont licenciées au niveau provincial. Elle s'appliquerait à toutes les organisations et activités à l'exception de celles qui sont régies par la législation s'appliquant au secteur public et des organisations traditionnellement sous juridiction fédérale (les banques, les entreprises de câblodistribution, etc).

*« Il est essentiel de disposer d'une loi complète à cet égard, pour protéger la liberté de choix et la vie privée de toute la population ontarienne. »*

Rapport annuel 1999 du Dr Ann Cavoukian, Commissaire à l'information et à la protection de la vie privée de l'Ontario

Une loi sur la protection des renseignements personnels, en Ontario, pourrait aussi étendre cette protection au delà des seules activités commerciales comme ce serait le cas si, en l'absence d'une législation ontarienne, seule la législation fédérale devait s'appliquer. Par exemple, de nombreuses organisations sans but lucratif utilisent des données personnelles à des fins non commerciales et, dans toutes les organisations, les employeurs les utilisent de façon interne. L'Ontario et le gouvernement fédéral doivent tous deux agir pour établir une protection complète de ces renseignements personnels.

**Objectif 2. Flexibilité pour des besoins et des circonstances uniques en matière de protection des renseignements personnels**

Il est primordial de disposer de données opportunes et exactes pour pouvoir prendre les bonnes décisions dans le domaine de santé, alors que les données sur la santé des particuliers soient très personnelles et que la vie privée de ces derniers doive être protégée. La loi sur la protection des renseignements personnels, proposée par l'Ontario, comprendrait des règles de protection s'appliquant spécifiquement aux données personnelles sur la santé des particuliers. Ces règles s'appliqueraient aussi bien dans le secteur public que dans le secteur privé. Le ministère de la Santé et des Soins de longue durée procédera à une consultation, plus tard au cours de l'été, sur les règles de protection des données personnelles en matière de santé et il espère bien bénéficier de vos commentaires sur la question. Vous trouverez, à l'annexe B, d'autre information sur la protection des données personnelles en matière de santé, ou vous pouvez appeler au ministère de la Santé et des Soins de longue durée.

La loi sur la protection des renseignements personnels, proposée par l'Ontario, établirait aussi un processus rigoureux de développement de codes sectoriels. Un code sectoriel est un ensemble de règles permettant d'ajuster les exigences de la loi proposée à une industrie ou à un type de renseignements donnés, ou encore à une façon donnée d'utiliser des renseignements. Ces codes permettraient ainsi de répondre aux besoins du public dans des organisations ou des secteurs particuliers ou encore pour des types particuliers de renseignements personnels.

L'application de règles particulières pourrait être appropriée, par exemple, dans les domaines des dossiers d'employé(e)s et de l'utilisation des données personnelles à des fins de rapport de crédit, ce dernier domaine étant actuellement couvert par la *Loi sur les renseignements concernant le consommateur.*

**Objectif 3. Application juste et efficace**

Une législation provinciale pourrait fournir des règles pratiques pour une grande variété d'organisations y compris de petites entreprises qui n'utilisent pas de données personnelles d'une manière courante ou qui font affaire d'un bout à l'autre du pays. Ces règles s'appliqueraient de façon claire et bien délimitée et elles refléteraient l'esprit de la norme CSA sans imposer de fardeau exagéré en matière de réglementation.

Une telle législation ferait beaucoup pour promouvoir la confiance à l'égard de la « place d'affaires Ontario » et des organisations de la province, en même temps que de maximiser les chances de succès de cette dernière dans une économie de plus en plus numérisée.

**Objectif 4. Compatibilité avec les autres lois**

La loi sur la protection des renseignements personnels, proposée par l'Ontario, se baserait sur la norme CSA et ressemblerait, dans sa substance, à la législation fédérale. Son application serait clairement définie de façon à éviter tout chevauchement avec d'autres lois provinciales comme la *Loi sur l'accès à l'information et la protection de la vie privée* et la *Loi sur l'accès à l'information municipale et la protection de la vie privée.* Elle ne primerait pas sur les dispositions de lois comme la *Loi sur l'éducation* ou la *Loi sur les services à l'enfance et à la famille.*

**Comment une loi ontarienne et la loi fédérale sur la protection des renseignements personnels pourraient-elles coexister?**

La loi sur la protection des renseignements personnels, proposée par l'Ontario, compléterait les aspects de la loi fédérale portant sur la conduite requise des organisations ainsi que sur les droits des particuliers. Par conséquent, le gouvernement fédéral accorderait probablement une exemption pour toutes les questions régies par la loi ontarienne proposée.

La plupart des entreprises, ayant leurs activités en Ontario, n'auraient à se préoccuper que de la loi ontarienne. Les organisations qui échangent des données personnelles à l'extérieur de l'Ontario, seraient encore assujetties à la législation fédérale comme le sont les organisations traditionnellement sous juridiction fédérale. La similitude entre la loi sur la protection des renseignements personnels, proposée par l'Ontario, et la législation fédérale est telle qu'elle empêcherait les chevauchements occasionnels de devenir des sources de conflit ou de confusion.

L'Ontario collaborera étroitement avec le gouvernement fédéral et les autres juridictions pour harmoniser ces lois.

## L'approche proposée par l'Ontario reflète la norme CSA

L'Ontario appuie sans restriction la norme CSA. De fait, l'Ontario est la seule province qui a participé à l'élaboration du Code type sur la protection des données personnelles de la CSA.

La loi sur la protection des renseignements personnels, proposée par l'Ontario, sera basée sur la norme CSA. Cependant, bien que la norme CSA convienne bien à une application en tant que norme volontaire, tous ses éléments ne se prêtent peut-être pas à législation. Par conséquent, l'Ontario étudie séparément chaque élément de la norme CSA pour décider s'il pourrait ou non constituer une exigence statutaire.

Dans certains cas, la norme CSA repose sur des recommandations pour des processus de gestion d'information. La législation proposée par l'Ontario serait axée sur les résultats et sur des exigences claires plutôt que sur des processus. En d'autres mots, si les principales dispositions de la norme CSA devaient être adoptées, certaines autres ne seraient pas utilisées dans la loi sur la protection des renseignements personnels, proposée par l'Ontario.

Cette ébauche d'approche s'écarte de la conception de la loi fédérale, mais la loi proposée serait tout de même très similaire à la loi fédérale, en ce qui concerne les principaux éléments de la norme CSA. La loi proposée serait ébauchée sur le modèle de la législation québécoise en matière de protection des renseignements personnels, laquelle est en place depuis 1994 et joue son rôle de façon satisfaisante.

Plus loin dans ce document, vous aurez à répondre si vous êtes ou non d'accord avec cette approche.

## Quels seraient vos droits en vertu de cette loi sur la protection des renseignements personnels, proposée par l'Ontario?

D'une manière générale, la loi sur la protection des renseignements personnels, proposée par l'Ontario, vous garantirait trois choses, en tant que particulier :

1. Vous pourriez mieux contrôler quand et comment vos données personnelles seraient recueillies, utilisées et divulguées.

2. Vous pourriez avoir accès à vos données personnelles et les modifier au besoin.

3. Vous auriez la possibilité de porter plainte, advenant que vos données personnelles soient recueillies, utilisées ou divulguées en contravention avec la loi.

### Vos droits avant la cueillette de vos données personnelles

En vertu de la loi sur la protection des renseignements personnels, proposée par l'Ontario, vous auriez à donner votre consentement avant toute cueillette de vos données personnelles. N'importe quelle organisation devrait expliquer quel genre de données personnelles elle voudrait obtenir et pourquoi. Une organisation qui prévoirait de communiquer vos données personnelles à un tiers, devrait d'abord vous expliquer à quel genre de tiers et pour quelles raisons, à la suite de quoi, vous donneriez ou non votre consentement.

Votre consentement serait généralement « express » -- en signant un document ou en remplissant un formulaire électronique par exemple. La loi proposée ne permettrait qu'un consentement « tacite » dans des circonstances raisonnables ou évidentes. Par exemple, il serait raisonnable qu'un journal estime avoir votre accord tacite pour utiliser votre adresse personnelle après que vous auriez acheté un abonnement avec livraison à domicile.

### Vos droits après la cueillette de vos données personnelles

La loi proposée vous donnerait aussi la possibilité de retirer votre consentement pour la cueillette, l'utilisation ou la divulgation de vos données personnelles. L'organisation impliquée devrait expliquer toutes les conséquences du retrait de votre consentement.

En revanche, la loi proposée ne vous permettrait pas de retirer votre consentement dans le but de briser un contrat. Par exemple, vous ne pourriez pas empêcher un créancier d'utiliser vos données personnelles en vue de collecter une dette que vous auriez contractée et qui serait due.

Advenant que vos données personnelles aient été communiquées à un tiers, l'organisation responsable serait dans l'obligation de vous aider à identifier ce tiers, afin que vous puissiez éventuellement signifier à ce dernier votre refus de le laisser utiliser vos données personnelles.

En vertu de la loi proposée, l'on ne pourrait pas vous refuser une marchandise, un service ou toute autre transaction sous prétexte que vous auriez refusé de fournir des données personnelles pour un usage sans relation avec la transaction.

**Qui peut donner un consentement?**

Un point important à prendre en considération est l'âge minimum à partir duquel un mineur peut donner ou refuser de donner lui-même son consentement. En Ontario, l'âge de la majorité est 18 ans; dans la mesure où la loi ne précise pas si et quand le mineurs peuvent donner ou refuser eux-même leur consentement à la cueillette et à l'utilisation de leurs données personnelles, cela entraînera immanquablement des doutes sur la validité du consentement donné par des mineurs dans des transactions comme s'abonner à un magazine ou prendre une carte de membre dans un club.

La loi sur la protection des renseignements personnels, proposée par l'Ontario, pourrait donner aux mineurs, à partir d'un certain âge qui pourrait être 13 ans, la capacité de donner eux-mêmes leur consentement pour la cueillette et l'utilisation de leurs données personnelles, ce qui leur permettrait d'avoir accès à l'emploi et de se lancer dans des activités commerciales. Le code de déontologie des commerçants canadiens ainsi que la législation américaine sur la protection des renseignements personnels appliquée à l'utilisation de l'Internet par les mineurs, ont adopté l'âge de 13 ans comme âge minimum. De plus, les jeunes peuvent généralement commencer à travailler dès l'âge de 14 ans. S'ils n'avaient pas alors la capacité de consentir eux-mêmes à fournir leurs données personnelles à des employeurs potentiels, cela pourrait affecter leur capacité de recherche d'emploi.

La loi proposée pourrait établir un âge à partir duquel les mineurs auraient la capacité de donner ou de refuser eux-même leur consentement à la cueillette et à l'utilisation de leurs données personnelles; cette capacité, cependant, se limiterait à la circonstance particulière pour laquelle le consentement serait requis; pour toute autre raison qui ne serait pas directement reliée, incluant toutes divulgations ultérieures, le consentement des parents serait requis. Pour les mineurs d'un âge inférieur à l'âge établi, le consentement des parents serait toujours requis.

Cependant, la loi proposée ne changerait pas l'âge du consentement pour utilisation de données personnelles stipulé dans une autre loi.

Une personne qui, de façon statutaire, serait autorisée à agir au nom d'une autre personne, serait aussi en mesure de donner ou de refuser son consentement au nom de cette autre personne.

Voici la première de nos 13 questions. Ces questions portent sur des propositions en vue d'une loi générale sur la protection des renseignements personnels et ne s'appliquent pas aux renseignements personnels dans le domaine de la santé.
Nous vous demandons d'expliquer si oui ou non vous soutenez le sujet que couvre la question et de faire tous autres commentaires que vous jugerez appropriés. Vous n'avez pas à vous limiter à ce seul sujet; les commentaires plus généraux seront aussi les bienvenus. Vous trouverez un formulaire qui pourra vous aider.

**<u>Question 1</u> : La loi proposée sur la protection des renseignements personnels devrait-elle inclure des règles établissant quand des mineurs peuvent donner leur consentement?**

Oui, la loi proposée devrait inclure des règles établissant quand des mineurs peuvent ou ne peuvent pas donner leur consentement.

Si oui, à partir de quel âge croyez-vous qu'un mineur devrait pouvoir donner ou refuser de donner son consentement?

Non, la Loi sur la protection des renseignements personnels ne devrait pas comporter de règles établissant si oui ou non des mineurs peuvent donner leur consentement.

**Cueillette indirecte**

Il arrive souvent que des données personnelles soient fournies par un tiers plutôt que par la personne concernée. En d'autres mots, une personne ne donnant pas directement ses données personnelles ne peut pas donner son consentement. Par exemple, si vous faites livrer des fleurs à quelqu'un, vous donnerez au fleuriste le nom et l'adresse de la personne à qui vous voulez les faire livrer. Il existe bien d'autres exemples de cueillette indirecte de données personnelles sans consentement : quelqu'un qui fait des réservations de voyage pour un(e) ami(e), ou qui achète un livre ou un abonnement à un magazine comme cadeau et le fait livrer à domicile, etc.

Beaucoup de ces activités sont personnelles ou familiales et impliquent des organisations qui seraient normalement tenues de respecter les règles d'obtention de consentement qu'imposerait la loi, pour recueillir et utiliser des données personnelles.

Si la loi proposée n'apportait pas de solution à cette question de cueillette indirecte, cela risquerait de provoquer beaucoup de confusion. Les gens pourraient s'inquiéter des risques d'utilisation abusive de cette cueillette indirecte sans consentement. La loi proposée pourrait définir des situations limitées dans lesquelles la cueillette indirecte de données personnelles sans consentement serait autorisée.

Ainsi la cueillette indirecte de données personnelles ne serait pas autorisée dans des cas où la personne concernée pourrait raisonnablement ne pas donner son consentement ou juger cette cueillette ou cette utilisation non désirable.

**<u>Question 2</u> : La loi sur la protection des renseignements personnels, proposée par l'Ontario, devrait-elle inclure des règles pour la cueillette indirecte de données personnelles sans consentement?**

Oui, la loi sur la protection des renseignements personnels, proposée par l'Ontario, serait plus claire si elle décrivait certaines situations limitées dans lesquelles serait autorisée la cueillette indirecte de données personnelles sans consentement.

Non, la question de cueillette indirecte devrait être traitée différemment.

Si non, comment la loi sur la protection des renseignements personnels, proposée par l'Ontario, devrait-elle aborder les règles de cueillette indirecte?

**Vos droits sur vos propres données personnelles**

En vertu de la loi sur la protection des renseignements personnels, proposée par l'Ontario, vous auriez le droit de consulter vos données personnelles, incluant celles qui auraient été enregistrées avant que la loi soit adoptée. Vous auriez aussi le droit de savoir si et comment ces données seraient utilisées ou bien communiquées à d'autres organisations.

Comme dans n'importe quelle loi, la raison prévaudrait. Une organisation ne serait pas obligée de divulguer des secrets commerciaux, ou de violer le secret professionnel de l'avocat, ou encore de faire prendre des risques à quelqu'un pour honorer votre demande d'accès à vos données personnelles.

En vertu de la loi sur la protection des renseignements personnels, proposée par l'Ontario, vous auriez aussi la possibilité de corriger des données personnelles inexactes. En cas de désaccord non résolu sur l'exactitude de vos données personnelles, vous auriez le droit d'exiger que les données que vous jugez inexactes soient identifiées comme telles; un bon exemple serait un contentieux non résolu entre une organisation et un particulier à propos d'une dette en souffrance. Une législation sur la protection des renseignements personnels n'est ni appropriée ni pratique pour résoudre ce genre de dispute; des données personnelles remises en question peuvent tout de même être identifiées en conséquence.

**Votre organisation utilise des données personnelles -- Quelles seraient ses obligations en vertu de la loi proposée?**

En vertu de la loi sur la protection des renseignements personnels, proposée par l'Ontario, votre organisation serait tenue de respecter le contrôle d'un particulier sur la confidentialité de ses données personnelles.

*Les firmes et organisations de l'Ontario seront avantagées si la province acquiert la réputation d'une juridiction qui protège la vie privée.*

La cueillette de données personnelles devrait inclure la transformation de données en apparence anonymes en données personnelles, par l'analyse ou la combinaison de données.

**La loi proposée s'appliquera-t-elle quel que soit le type d'organisation?**

La protection des renseignements personnels n'est pas une préoccupation seulement dans le monde du commerce. Beaucoup de domaines d'activités non commerciales impliquent des données personnelles qui devraient, elles aussi, bénéficier des règles de protection des renseignements personnels. Par exemple, les oeuvres de bienfaisance, les universités, les organisations syndicales, les associations professionnelles, les organisations religieuses et les groupes de revendication peuvent recueillir des données personnelles. Cela veut dire que la proposition d'une loi ontarienne sur la protection des renseignements personnels intéresse un large éventail d'organisations.

La loi sur la protection des renseignements personnels, proposée par l'Ontario, s'appliquerait à l'ensemble du monde des affaires, aux organisations sans but lucratif, à l'exception des organisations régies par la législation s'appliquant au secteur public et des organisations sous juridiction fédérale (comme les banques et les télécommunications). Certaines activités seraient exemptées comme la cueillette, l'utilisation et la divulgation de données personnelles à des fins de maintien de l'ordre. Ces propositions d'exemptions sont abordées plus loin dans ce document.

La loi sur la protection des renseignements personnels, proposée par l'Ontario, ne s'appliquerait pas à l'utilisation de données personnelles à des fins personnelles, familiales ou domestiques comme l'utilisation de votre liste de noms et d'adresses pour envoyer des cartes de voeux.

**Comment votre organisation se conformerait-elle à la loi proposée?**

La loi sur la protection des renseignements personnels, proposée par l'Ontario, impliquerait cinq devoirs découlant de la norme CSA. À l'égard de toute personne concernée, votre organisation serait normalement tenue de :

1. L'informer des données personnelles que vous voulez recueillir et pour quelles raisons.
2. Obtenir son consentement pour la cueillette, l'utilisation et la divulgation de ses données personnelles.
3. Recueillir, utiliser et divulguer ses données personnelles selon les règles établies dans la loi.
4. Lui donner accès à ses données personnelles et corriger les données inexactes lorsqu'elle en fait la demande.
5. Garder ces données personnelles en sécurité et en disposer de façon appropriée.

En vertu de la loi proposée, votre organisation serait seulement autorisée à recueillir, utiliser ou divulguer des données personnelles pour des raisons que la personne concernée jugerait appropriées, dans les circonstances. Par exemple, il n'est pas raisonnable de recueillir des données de nature raciale ou religieuse lors d'une transaction pour laquelle la législation sur les droits de la personne interdit de prendre une décision sur la base de telles données.

La loi proposée n'obligerait pas les organisations à suivre des étapes de procédure comme celles qui sont définies dans le principe de responsabilisation de la norme CSA, incluant la mise en oeuvre d'un programme de formation du personnel et l'élaboration d'une politique de protection des renseignements personnels. Ces procédures sont de bonnes pratiques d'affaires mais elles ne seraient pas obligatoires en vertu de la loi proposée.

**De quelle manière votre organisation devrait-elle recueillir des données personnelles?**

En vertu de la loi sur la protection des renseignements personnels, proposée par l'Ontario, vous devriez normalement informer une personne que votre organisation désire recueillir des données la concernant et obtenir son consentement pour cela.

Votre organisation devrait décrire de façon compréhensible le but de cette cueillette. Si ce but est de faire la mise en marché de produits, il ne suffirait pas de dire qu'il s'agirait de « mise en marché »; il faudrait aussi préciser les types de produits ou le genre de détaillants. Par exemple, vous pourriez dire à la personne concernée que ses données personnelles seraient utilisées dans la mise en marché de produits qui semblent l'intéresser, selon une enquête sur les préférences des consommateurs à laquelle elle aurait répondu.

En vertu de la loi proposée, au cas où ce ne serait pas évident, votre organisation serait tenue de préciser à la personne concernée quelles données personnelles elle compterait recueillir et de quelle manière elle les recueillerait (en interrogeant d'autres organisations sur la personne concernée, par exemple).

Votre organisation serait aussi tenue de dire à la personne concernée si elle aurait l'intention de communiquer ces données personnelles à un tiers. L'explication devrait établir clairement à quel genre de tiers les données personnelles seraient communiquées et pour quelles raisons.

Ces explications devraient être fournies avant ou au moment de la cueillette des données.

**De quelle manière votre organisation peut-elle obtenir un consentement?**

En vertu de la loi proposée, votre organisation solliciterait un consentement sur une action ou un document spécifique ou encore par le biais de dispositions dans un contrat ou sur un formulaire de demande d'emploi, documents dans lesquels on demande habituellement à une personne d'accepter le tout par une seule et unique signature. Tout consentement pourrait couvrir divers buts et usages futurs, dans la mesure où ces derniers auraient été clairement établis et décrits auparavant.

Un consentement pourrait être obtenu verbalement, par écrit ou électroniquement selon ce qui serait le plus approprié dans les circonstances.

La loi proposée exigerait normalement que votre organisation obtienne un consentement directement de la personne concernée. Il est proposé, cependant, qu'une autre organisation pourrait obtenir un consentement pour votre organisation, dans la mesure où elle aurait préalablement identifié cette dernière comme un tiers à qui elle aurait prévu de communiquer les données personnelles en question. En d'autres termes, si une personne donnait son consentement après avoir été informée que ses données personnelles pourraient être communiquées à une tierce organisation comme la vôtre, l'organisation qui aurait fait la demande pourrait alors communiquer les données personnelles en question à votre organisation. De façon similaire, votre organisation pourrait divulguer des données personnelles à une autre organisation, dans des circonstances analogues (votre organisation ayant obtenu un consentement pour le faire).

Un consentement serait permis, pourvu qu'existe une option de refus clairement indiquée dans un contrat, sur un formulaire de demande d'emploi ou autre (c.-à-d., sous la forme d'une case à cocher pour empêcher l'utilisation ou la divulgation des données personnelles vous concernant). Une option de refus pourrait être mise en place par le biais d'un document sur lequel une personne concernée devrait de toute façon donner son accord ou par le biais d'une note claire établissant des moyens directs (et gratuits) d'exercer cette option. Il ne serait pas acceptable qu'une organisation dispose seulement d'une politique permettant de refuser en cas de demande explicite, sans faire le nécessaire pour que les personnes concernées soient averties de l'existence d'une telle option et disposent d'un moyen facile de l'exercer.

La norme CSA ne traite de cette option de refus qu'en termes généraux. La loi sur la protection des renseignements personnels, proposée par l'Ontario, clarifierait l'utilisation du consentement avec option de refus, afin d'éviter les risques de dispute.

**<u>Question 3</u> : Est-ce qu'une option de refus devrait être clairement autorisée comme élément de contrat, d'entente ou d'avis?**

Oui, la législation devrait limiter, tel que proposé, l'utilisation du consentement avec option de refus.

Non, la législation devrait établir des règles différentes d'utilisation de cette option (moins/plus contraignantes).

Si non, la législation devrait-elle avoir plus ou moins de règles pour utiliser l'option de refus?

**Est-ce que votre organisation peut décider de ne pas traiter avec quelqu'un qui refuse de donner son consentement?**

En vertu de la loi sur la protection des renseignements personnels, proposée par l'Ontario, votre organisation pourrait décider de ne pas traiter avec quelqu'un qui refuserait de donner son consentement, dans la mesure où les données personnelles en question seraient effectivement nécessaires à la transaction.

Cependant, si les données personnelles en question n'auraient aucune relation avec la transaction, votre organisation n'aurait pas le droit de les demander pour compléter la transaction. La personne concernée serait encore en droit d'acheter vos produits, par exemple, ou de s'inscrire à votre club sans pour autant permettre à votre organisation de communiquer ses nom et adresse à un tiers pour un autre usage. Cela veut dire qu'une personne pourrait refuser de donner son consentement, dans le cadre d'un contrat, d'une demande d'emploi ou de toute autre formule d'entente, à une utilisation de ses données personnelles qui ne serait pas directement reliée à ce contrat, cette demande d'emploi ou cette autre formule d'entente.

La disposition de la norme CSA sur la demande de consentement, couvre seulement la fourniture de produits et de services, tandis que la loi proposée couvrirait toutes les transactions y compris, par exemple, les ententes entre propriétaires et locataires ainsi que les transactions non commerciales.

**Dans quelles circonstances mon organisation pourrait-elle se servir du « consentement tacite »?**

Un consentement tacite pourrait économiser du temps aux personnes concernées et aux organisations. La loi sur la protection des renseignements personnels, proposée par l'Ontario, autoriserait un consentement tacite seulement dans les situations où l'identification expresse des buts de votre organisation et l'obtention d'un consentement ne seraient pas une nécessité. Un consentement tacite ne s'appliquerait qu'à des données personnelles directement reliées à une transaction et il faudrait encore obtenir le consentement de la personne concernée pour toute autre utilisation ou divulgation de ces données.

*Votre entreprise d'enlèvement de la neige pourrait envoyer, à l'automne, à tous ses clients de l'année précédente, une lettre leur offrant vos services pour cette année. Cependant, vous seriez dans l'obligation de respecter les désirs de clients qui vous auraient demandé, l'année précédente, de ne plus leur envoyer de courrier.*

Ainsi, l'on pourrait raisonnablement s'attendre à ce qu'une organisation conserve des dossiers financiers et de contrôle de qualité sur ses transactions. Ces dossiers ne sont normalement pas divulgués à l'extérieur de l'entreprise et, d'ordinaire, n'ont aucun lien avec la personne concernée. Votre organisation pourrait s'appuyer sur un consentement tacite pour se servir de ces données, en vertu de la loi proposée.

Ce que l'on propose, c'est que lorsqu'un consentement tacite est approprié, votre organisation n'aurait pas à informer expressément les personnes concernées de la raison pour laquelle vous recueillez des données personnelles ni à leur demander expressément leur consentement.

Cependant, si une personne concernée le demandait, votre organisation devrait fournir toutes les explications sur la façon dont ses données personnelles auraient été utilisées ou divulguées.

En vertu de la loi proposée, une personne pourrait encore refuser de donner son consentement dans la plupart des situations où un consentement tacite s'applique, auquel cas votre organisation pourrait raisonnablement refuser de conclure la transaction. Un consentement tacite concerne généralement des données qui sont nécessaires à une transaction; il ne serait donc pas raisonnable de conclure une transaction sans avoir obtenu ces données. Par exemple, une entreprise ne peut être empêchée de tenir des dossiers de vérification interne ni de donner une adresse à ses livreurs.

Cependant, en vertu de la loi proposée, un simple consentement tacite ne suffirait pas pour la divulgation de données personnelles à un tiers. De même, un simple consentement tacite ne permettrait pas de recueillir des données personnelles auprès d'une quelconque source autre que la personne concernée elle-même ou sans que cette dernière en ait connaissance. Enfin, un simple consentement tacite ne s'étendrait pas à la promotion, auprès d'un client, de produits ou de services additionnels ou différents.

**Question 4 : Est-ce que la loi devrait définir des circonstances limitées dans lesquelles un consentement tacite serait approprié, comme des transactions qui n'impliquent qu'une utilisation interne et limitée de données personnelles?**

Oui, la loi devrait prévoir des circonstances limitées dans lesquelles un consentement tacite serait autorisé comme l'utilisation uniquement interne des données personnelles.

Non, la loi devrait aborder le consentement tacite de façon différente.

Si non, la loi devrait-elle définir l'utilisation du consentement tacite d'une façon plus large ou plus étroite? Par exemple, devrait-elle permettre à une organisation de se servir des données personnelles pour faire la promotion de produits ou de services non connexes?

**Est-ce que mon organisation serait limitée dans son utilisation des données personnelles?**

En vertu de la loi sur la protection des renseignements personnels, proposée par l'Ontario, des limites raisonnables seraient établies. Par exemple, si votre organisation changeait ses plans et voulait utiliser des données personnelles à d'autres fins que celles déjà expliquées à la personne concernée, ou qu'elle voulait recueillir d'autres données en plus de celles déjà identifiées, elle devrait obtenir un nouveau consentement pour toute nouvelle cueillette, utilisation ou divulgation.

Votre organisation pourrait utiliser, sans consentement express, de l'aide extérieure pour des tâches comme faire du traitement de données ou mener des campagnes de promotion ou de levée de fonds. Les données personnelles ne pourraient être utilisées que si la personne concernée a consenti à une telle utilisation ou si elle est autorisée en vertu de la loi proposée. Votre organisation et la firme extérieure seraient toutes deux responsables de ce qui serait fait avec ces données.

En vertu de la loi sur la protection des renseignements personnels, proposée par l'Ontario, votre organisation devrait maintenir des dossiers sur les divulgations de données personnelles à des tiers. Cela signifie que votre organisation pourrait, sur demande, permettre à des particuliers d'accéder à

ces données. Il ne serait pas nécessaire d'enregistrer toutes les divulgations pour chaque transaction, du moment que les arrangements faits par votre organisation seraient raisonnablement documentés.

**Quelles sont les obligations de mon organisation en ce qui concerne la conservation ou l'élimination de données personnelles?**

En vertu de la loi sur la protection des renseignements personnels, proposée par l'Ontario, votre organisation pourrait conserver des données personnelles aussi longtemps qu'il serait nécessaire pour atteindre les buts auxquels il a été consenti et pour se conformer à toute obligation de conservation de dossiers imposée par la loi. Votre organisation devrait disposer des dossiers soit en les détruisant soit en les rendant complètement anonymes. Votre organisation pourrait s'acquitter de cette obligation en établissant un calendrier d'élimination des données.

Votre organisation serait aussi tenue de respecter la décision d'un particulier de retirer son consentement à l'utilisation de ses données personnelles. Un tel retrait de consentement ne pourrait pas être rétroactif et serait assujetti à des limites raisonnables.

Il pourrait s'avérer parfois difficile de disposer de données personnelles, car les vieux dossiers papier ne sont pas faciles à trouver ou se prêtent mal à une destruction partielle. Des données personnelles pourraient aussi faire partie d'un dossier duquel elles ne pourraient pas être extraites sans affecter la validité du reste du dossier comme un contrat ou tout autre document juridique. En vertu de la loi proposée, ces problèmes seraient traités dans le cadre de politiques de gestion de dossiers.

**Quelles mesures de protection mon organisation devrait prendre pour assurer la sécurité des données personnelles?**

La loi sur la protection des renseignements personnels, proposée par l'Ontario, exigerait que votre organisation établisse et applique des mesures de sécurité appropriées au niveau de sensibilité des données personnelles qu'elle détiendrait. Ces mesures devraient être suffisantes pour empêcher tout accès non autorisé ou toute publication, modification ou utilisation accidentelle ou inopportune.

En vertu de la loi proposée, votre organisation devrait dévoiler ses mesures de protection à toute personne habilitée à recevoir une telle information, comme des clients potentiels par exemple. Le dévoilement, pour le public, de ces mesures de protection ne devrait pas être précis au point de mettre en danger la sécurité dans l'organisation. Par exemple, vous n'auriez pas à donner de détails sur votre sécurité Internet qui pourraient, par inadvertance, donner des idées à des pirates informatiques.

*Si vous vous servez d'Internet pour prendre un paiement par carte de crédit, vous pourriez avoir besoin d'identifier les mesures de sécurité utilisées, comme le chiffrement, par exemple. La loi proposée serait ébauchée de façon à assurer sa totale neutralité sur le plan technologique.*

Bien que la loi proposée n'adopterait pas le principe d'ouverture de la norme CSA, il serait néanmoins important que les pratiques d'une organisation soient visibles et compréhensibles pour les particuliers. En exigeant qu'une organisation dévoile ses mesures de protection, en plus de décrire ses sources de données personnelles ainsi que les autres organisations auxquelles elle les auraient divulguées, la loi proposée s'assurerait que les pratiques d'une organisation en matière de protection des renseignements personnels soient tout à fait limpides.

**<u>Question 5</u> : Est-ce que les organisations seraient obligées de dévoiler leurs mesures de protection?**

Oui, la loi proposée devrait clairement exiger que les organisations dévoilent leurs mesures de sécurité.

Non, il n'est pas nécessaire que la loi proposée oblige les organisations à dévoiler leurs mesures de sécurité.

**Qu'arriverait-il lorsqu'un particulier demanderait à avoir accès à des données personnelles?**

D'une façon générale, la loi proposée exigerait que votre organisation honore une demande d'accès. Votre organisation serait aussi tenue de permettre qu'une personne puisse mettre à jour ou corriger des données erronées ou inexactes et identifier des données litigieuses. Votre organisation devrait aussi être prête à dévoiler les sources auprès desquelles elle aurait recueilli ces données personnelles, ainsi que les autres organisations auxquelles elle les aurait communiquées.

La loi proposée refléterait le principe d'exactitude de la norme CSA, mais soulignerait que cette obligation juridique d'exactitude obligerait aussi à enregistrer tous les désaccords non résolus. En général, un problème significatif d'exactitude se manifesterait sous la forme d'une demande de correction de données personnelles ou d'un retrait de consentement. Alors que la loi résoudrait ces problèmes, elle ne devrait pas se transformer en forum pour résoudre les disputes sur les bases factuelles d'une information comme les dettes existantes.

Dans des situations où des données personnelles seraient utilisées pour rejeter une demande de produit ou de service par un particulier (par exemple, son dossier de crédit), votre organisation serait tenue d'informer le particulier, qu'elle pourrait bien revoir ses données personnelles pour s'assurer de leur exactitude.

Lorsqu'un particulier demanderait à revoir ses données personnelles, la loi proposée exigerait que votre organisation fournisse les données dans les 30 jours ou qu'elle informe le particulier qu'elle ne serait pas en mesure de les lui fournir, en vertu d'une exemption contenue dans la loi.

Il y aurait des limites raisonnables à l'obligation faite à votre organisation d'accorder un accès demandé; limites similaires à celles imposées dans les cas où votre organisation ne serait pas tenue de détruire des données personnelles (comme lorsqu'elles s'avéreraient difficiles à localiser).

En vertu de la loi proposée, votre organisation pourrait faire payer un droit pour le recouvrement des coûts d'accès à des données personnelles. Cependant, dans la mesure où les données personnelles auraient été utilisées pour refuser d'accorder un avantage ou pour augmenter le montant demandé, les personnes concernées seraient en droit de revoir leurs données gratuitement.

La loi sur la protection des renseignements personnels, proposée par l'Ontario, fournirait des moyens d'empêcher les abus de demandes importunes (comme lorsqu'une personne fait une demande chaque semaine pour revoir des données qui ne changent qu'une fois par an).

**<u>Question 6</u> : Est-ce que les droits d'accès et la résolution des problèmes d'exactitude qui sont proposés, sont appropriés?**

Oui, l'accent que la loi proposée met sur l'accès, la correction des données inexactes et l'identification des données litigieuses, est approprié.

Non, l'exactitude des données personnelles devrait faire l'objet d'une exigence statutaire.

**Est-ce que mon organisation pourrait déplacer des données hors de l'Ontario?**

La loi sur la protection des renseignements personnels, proposée par l'Ontario, n'empêcherait pas des organisations de déplacer des données à l'intérieur ou à l'extérieur du Canada.

À l'intérieur du Canada, la *Loi* fédérale *sur la protection des renseignements personnels et les documents électroniques* s'appliquerait aux utilisations commerciales. Les lois d'autres provinces, sur la protection des renseignements personnels, pourraient aussi s'appliquer dans la mesure où elles existeraient.

En vertu de la loi proposée, si votre organisation devait divulguer des données personnelles en dehors du Canada, en particulier des données non commerciales pas couvertes par la législation fédérale, elle devrait prendre des mesures raisonnables pour assurer que les dispositions de la loi sur la protection des renseignements personnels, proposée par l'Ontario, seraient respectées. Cela pourrait inclure l'ajout de dispositions à des contrats pour assurer que les données personnelles ne seraient utilisées que dans les buts déjà identifiés et pour lesquels il y aurait eu consentement.

**<u>Question 7</u> : Est-ce que la loi proposée devrait couvrir la question du déplacement de données à l'extérieur de l'Ontario?**

Oui, la loi sur la protection des renseignements personnels, proposée par l'Ontario, devrait inclure des règles sur l'utilisation contractuelle de mesures de protection pour assurer une protection adéquate de la vie privée lorsque des données sont communiquées à une autre juridiction.

Non, la loi sur la protection des renseignements personnels, proposée par l'Ontario, ne devrait pas couvrir les besoins de protection des renseignements personnels en dehors de sa juridiction.

**Que devrait faire mon organisation en ce qui concerne les dossiers existants de données personnelles?**

En vertu de la loi sur la protection des renseignements personnels, proposée par l'Ontario, votre organisation serait tenue de respecter ses obligations à l'égard de toutes les données personnelles y compris les dossiers existants.

La période de transition proposée, pour une nouvelle loi sur la protection des renseignements personnels, serait probablement de douze mois. Au cours de cette période, votre organisation devrait revoir les données personnelles qu'elle détiendrait et dont l'utilisation aurait déjà reçu un consentement.

Si votre organisation voulait continuer à utiliser des données personnelles existantes ou les divulguer à d'autres, elle devrait sans doute entrer en contact avec les personnes concernées pour leur fournir les explications appropriées et obtenir leur consentement.

**Question 8 : La proposition d'une transition avant l'entrée en vigueur de la Loi est-elle appropriée?**

Oui, la proposition d'une période de transition est raisonnable.

Non, les dispositions relatives à la transition devraient être différentes.

**Évaluation de l'approche proposée de manière à refléter la norme CSA**

À ce point, nous aimerions entendre vos commentaires sur notre approche jusqu'à maintenant.

La loi sur la protection des renseignements personnels, proposée par l'Ontario, tente de réaliser un équilibre entre une préoccupation intense du public quant à la protection des renseignements personnels et les avantages que procure un régime de réglementation clair qui s'harmonise bien avec la loi fédérale.

En vertu de la loi proposée, les organisations seraient tenues légalement responsables de se plier aux règlements proposés de protection des renseignements personnels, et il leur appartiendrait de mettre en œuvre les étapes leur permettant de se conformer à la loi. Les questions organisationnelles telles que la formation du personnel ne pourraient pas faire l'objet d'enquêtes ou de plaintes.

Cette approche diffère de la loi fédérale. Or, la loi fédérale et la loi sur la protection des renseignements personnels, proposée par l'Ontario, s'inspirent toutes deux de la norme CSA et la loi proposée par l'Ontario emprunterait, le plus possible, sa terminologie et ses exigences.

Le reste du présent document porte sur la nécessité de donner de la souplesse à la loi proposée et de veiller à sa mise en application. Nous voulons combiner clarté avec capacité de souplesse future et mise en application efficace.

**Question 9 : L'approche adoptée pour la loi sur la protection des renseignements personnels, proposée par l'Ontario, réalise-t-elle un équilibre approprié entre une protection des renseignements personnels adéquate et des règlements clairs et applicables?**

Oui, l'approche de la loi sur la protection des renseignements personnels, proposée par l'Ontario, est bien inspirée.

Oui, l'approche de la loi sur la protection des renseignements personnels, proposée par l'Ontario, est bien inspirée dans l'ensemble, mais certaines modification sont souhaitables.

Non, une approche différente est recommandée.

**Conférer de la souplesse en fonction de besoins particuliers de protection des renseignements personnels**

La loi sur la protection des renseignements personnels, proposée par l'Ontario, doit être neutre d'un point de vue technologique et convenir à un grand éventail d'organisations et de types de données personnelles. Cependant, même si des règles générales convenaient à la plupart des organisations, des règlements spécialisés pourraient être nécessaires dans certains secteurs précis. La loi proposée serait dotée de deux mécanismes qui permettraient d'établir des normes de protection des renseignements personnels spécialisées.

- Une annexe à la loi proposée prescrirait des règlements pour la protection des renseignements personnels en fonction du secteur de la santé.

- Un processus serait ensuite mis sur pied pour établir et adapter les règlements de protection des renseignements personnels en fonction de secteurs ou de types de données personnelles particuliers.

**Règlements sur la protection des renseignements personnels dans le secteur de la santé**

De bons soins de santé dépendent de la disponibilité opportune des données. Les données individuelles sur la santé ne devraient cependant être partagées qu'à des fins légitimes et sanctionnées par la loi. Le ministère de la Santé et des Soins de longue durée a entrepris une consultation distincte concernant les modes acceptables de cueillette, d'utilisation ou de divulgation des données personnelles dans le secteur de la santé.

L'information au sujet des règlements proposés pour le secteur de la santé et de la façon de participer à la consultation menée par le ministère de la Santé et des Soins de longue durée se trouve à l'annexe B.

**Codes de secteur pour répondre à des besoins particuliers de protection des renseignements personnels**

La loi sur la protection des renseignements personnels, proposée par l'Ontario, prévoit l'utilisation, s'il y a lieu, de codes de secteur en fonction de besoins particuliers d'un secteur ou d'un type de données personnelles. Le code de secteur représente un ensemble de règles qui sont adaptées aux exigences de la loi proposée pour une industrie, un type de données personnelles ou une façon d'utiliser les données particulières.

Les codes de secteur aborderaient clairement les questions et les préoccupations précises d'un secteur ou d'une industrie en particulier, en détails plus appropriés que dans une loi générale. Les codes pourraient modifier l'application de certaines parties de la loi de manière à tenir compte des besoins d'un secteur ou d'une industrie en particulier et à mettre au point des pratiques d'information adaptées à des questions particulières. Un code de secteur pourrait se justifier dans une grande variété de domaines, par exemple, dans des secteurs économiques comme les services financiers ou pour un type particulier de données personnelles comme les dossiers d'employé(e)s.

La loi proposée mettrait en place un processus rigoureux et transparent qui permettrait d'élaborer ou de modifier un code de secteur. Le processus ferait appel à la participation de représentants du secteur, de l'intérêt public et d'experts, au besoin (comme dans le secteur juridique, technique, universitaire). Il aurait besoin de l'approbation finale du gouvernement.

Le secteur de l'évaluation du crédit serait par exemple un domaine où un code de secteur serait proposé. Il existe déjà des règlements qui régissent l'échange de données personnelles à des fins d'évaluation du crédit dans la *Loi sur les renseignements concernant le consommateur.* Il pourrait convenir de réserver un code de secteur à l'évaluation du crédit en vertu de la loi sur la protection des renseignements personnels, proposée par l'Ontario, plutôt que de régir ce domaine en vertu de la loi actuelle, de manière à ce qu'il n'y ait pas de chevauchement des lois et qu'elle soit plus facile à encadrer.

L'expérience dans d'autres sphères de responsabilités suggère qu'il n'y aurait pas un grand nombre de codes de secteur. Il faudrait des arguments irréfutables pour élaborer un code de secteur. Le code de secteur ne pourrait pas être simplement un mécanisme pour faire valoir les points de vue ou les intérêts d'un groupement au détriment d'un autre. Tout code devrait améliorer le contexte d'ensemble du régime de protection des renseignements personnels en Ontario.

**<u>Question 10</u> : La proposition de codes de secteur assujettis à un processus législatif est-elle bien inspirée?**

Oui, la proposition de codes de secteur assujettis à un processus législatif est bien inspirée.

Non, la loi sur la protection des renseignements personnels, proposée par l'Ontario, ne permettrait pas d'élaborer des codes de secteur comme il est suggéré. Le cas échéant, quels processus faudrait-il prévoir dans la loi pour permettre l'élaboration et l'approbation des codes de secteur?

Non, la loi sur la protection des renseignements personnels, proposée par l'Ontario, ne devrait pas permettre l'élaboration de codes de secteur.

**Quelles sont les exemptions et les exceptions qui s'appliqueraient?**

On propose que, dans certaines situations, il ne soit pas nécessaire d'exiger le consentement d'une personne pour cueillir, utiliser ou divulguer ses données personnelles. Les exemptions aux exigences de consentement ou d'accès dans la loi sur la protection des renseignements personnels, proposée par l'Ontario, devraient aider à garantir la santé et la sécurité de nos collectivités ou à équilibrer la protection des données personnelles avec d'autres droits essentiels comme la liberté d'expression.

Les exemptions proposées portent sur les mêmes questions que celles abordées dans la loi fédérale sur la protection des renseignements personnels afin d'éviter toute confusion entre les deux lois.

**Quand des données personnelles peuvent-elles être recueillies, utilisées ou divulguées sans le consentement de la personne concernée?**

**Application de la loi :** La loi proposée n'empêcherait pas les personnes ou les organisations de coopérer avec la force publique. Elle permettrait aussi à une personne ou à une organisation de divulguer des données personnelles aux organismes d'application de la loi s'il y avait des motifs raisonnables de soupçonner une infraction.

**Journalisme, art et littérature :** L'exemption proposée ne toucherait pas les autres recours judiciaires comme la diffamation ou le libelle. Le journalisme et les autres organisations du même genre ne seraient pas complètement exemptés. Un journal devrait encore devoir obtenir un consentement pour vendre sa liste d'abonnés.

**Le bien-être de la personne :** Un consentement ne serait pas nécessaire si l'utilisation des données personnelles serait de toute évidence dans le meilleur intérêt présumé de la personne concernée et que la volonté expresse de cette dernière ne pourrait pas être déterminée.

**Défense de droits contractuels par des instances du secteur privé :** L'exemption proposée n'occulterait pas les mesures de protection déjà prévues par la loi comme celles sur la protection des consommateurs en matière de recouvrement de dette.

**Information du domaine public :** L'exemption proposée s'appliquerait à l'information du domaine public (comme le registre des sociétés ou les archives judiciaires).

**Autorisation législative :** L'exemption proposée s'appliquerait dans le cas ou une autre loi, fédérale ou provinciale, conférerait l'autorité de cueillir, d'utiliser ou de divulguer des données personnelles.

**Secret professionnel de l'avocat :** L'exemption proposée respecterait le secret professionnel de l'avocat de manière à ce que les personnes puissent exercer les divers droits et actions en justice dont elles jouissent aujourd'hui.

**Fins historiques :** L'exemption proposée permettrait la conservation de dossiers d'importance historique ou archivistique.

**Dans quelles situations des personnes ne seraient-elles pas autorisées à accéder à leurs données personnelles?**

En vertu de la loi proposée, des personnes pourraient ne pas être autorisées à accéder à toutes leurs données personnelles dans les situations suivantes :

**Application de la loi :** Une organisation n'aurait pas à mettre une enquête en péril en révélant qu'elle a fourni des données personnelles à un organisme d'application de la loi.

**Secret professionnel de l'avocat :** Toute exemption ne s'appliquerait qu'aux données assujetties au secret professionnel.

**Intérêts personnels conflictuels :** Une personne n'aurait pas le droit d'accéder à ses données personnelles si le bien-être d'autrui pouvait être mis en jeu.

**Secrets commerciaux :** Une exemption s'appliquerait si l'accès aux données personnelles révèle des secrets commerciaux. L'identité d'une personne à qui une entreprise aurait divulgué des données personnelles et les raisons d'une telle divulgation, ne seraient pas considérées comme un secret commercial.

Les exemptions d'accès aux données personnelles exigeraient habituellement qu'autant de renseignements que possible soit divulgués, de manière à ne taire que les renseignements de nature délicate.

**Quelles seraient les exceptions prévues en vertu de la loi proposée?**

**Recherche :** en vertu de la loi proposée, une exception pour fin de recherche ne serait autorisée sur demande que dans le cas où le but d'une recherche supposerait l'accès à des données personnelles et qu'il n'est pas pratique d'obtenir le consentement de la personne. Par exemple, en vertu de la loi proposée sur la protection des renseignements personnels, les droits continueraient de s'appliquer pour une période de trente ans après la mort d'une personne, conformément à la *Loi sur l'accès à l'information et la protection de la vie privée.* Une exception pour fins de recherche pourrait être accordée s'il s'avérait difficile de trouver une personne qui consentirait à l'accès à de tels dossiers. La loi proposée exigerait que l'intérêt public dans l'autorisation de recherche soit pondéré avec celui de l'intérêt individuel dans la protection des renseignements personnels.

**Secrets commerciaux :** en vertu de la loi proposée, une demande pourrait être adressée suivant laquelle un risque pour la vie, la santé ou la sécurité d'un individu devrait avoir la primauté sur l'exemption d'accès en raison d'un secret commercial.

**<u>Question 11</u> : Les exemptions et les exceptions de la loi sur la protection des renseignements personnels, proposée par l'Ontario, sont-elles raisonnables?**

Oui, les exemptions et les exceptions de la loi sur la protection des renseignements personnels, proposée par l'Ontario, sont raisonnables.

Non, des exemptions ou des exceptions ne devraient pas être prévues dans certains domaines de la loi sur la protection des renseignements personnels, proposée par l'Ontario. Dans ce cas, quels seraient ces domaines?

Pouvez-vous penser à d'autres exemptions ou exceptions qui devraient être prévues dans certains domaines de la loi sur la protection des renseignements personnels, proposée par l'Ontario. Si oui, veuillez les décrire.

## Comment la loi sur la protection des renseignements personnels, proposée par l'Ontario, sera-t-elle appliquée?

De manière semblable à la loi fédérale, la loi sur la protection des renseignements personnels, proposée par l'Ontario, créerait un organisme particulier responsable de la conformité à la législation.

L'Ontario a pour objectif de n'avoir qu'un seul organisme responsable de la conformité à la législation provinciale touchant à la protection des renseignements personnels. Nous voulons obtenir une rétroaction sur les dispositions d'application qui sont appropriées aux règlements relatifs à la protection des renseignements personnels qui viseraient les entreprises ainsi que d'autres organisations.

La législation existante touchant le secteur public, y compris la *Loi sur l'accès à l'information et la protection de la vie privée* et la *Loi sur l'accès à l'information municipale et la protection de la vie privée* désignent le Bureau de la commissaire à l'information et à la protection des renseignements personnels de l'Ontario comme son organisme de surveillance indépendant. Le présent document ne cherche pas à obtenir des commentaires sur la législation du secteur public, non plus que sur ses mécanismes de surveillance.

Les points de vue du Bureau de la commissaire sont requis, sur les propositions faites dans le présent document, en particulier sur les pouvoirs de police appropriés.

On vous demandera à la fin de la présente section votre opinion sur chacune des questions ou chacun des pouvoirs de police proposés. Vos commentaires sur les propositions aideront à définir le rôle de l'organisme qui sera chargé d'assurer la conformité aux lois relatives à la protection des renseignements personnels en Ontario.

### Loi de nature réglementaire fructueuse

La loi sur la protection des renseignements personnels, proposée par l'Ontario, vise à mettre en place des règles claires et significatives, tout en évitant les lourdeurs administratives et des fardeaux réglementaires exagérés.

Les pratiques d'information équitable représentent de bonnes pratiques de gestion. Plusieurs compagnies chef de file adoptent de nouveaux principes de gestion des données personnelles. Nous croyons que la plupart des organisations verraient des avantages économiques à adopter rapidement les règlements établis dans la loi sur la protection des renseignements personnels, proposée par l'Ontario.

En se penchant sur l'expérience du milieu des affaires en ce qui touche l'observation de la loi relativement aux normes du marché, nous pouvons voir qu'une mise en application efficace vient compléter la législation. Tous les commerces de vente au détail sont assujettis à des lois comme la *Loi sur les pratiques de commerce* et la *Loi sur la protection du consommateur* et pourtant, la plupart des commerces, parce qu'ils sont préoccupés par le service à la clientèle, ne se sentent pas menacés par des enquêtes, des poursuites ou même des actions au civil en vertu de ces lois.

Seule une minorité d'organisations essaient sérieusement de violer la loi. La mise en application ferme de la loi vise particulièrement cette minorité. Le plus souvent, le monde des affaires appuie l'application de la loi et va même parfois jusqu'à la demander. Il perçoit la persistance à ne pas se conformer aux dispositions de la loi comme une tentative d'acquérir un avantage concurrentiel injuste et un risque d'atteinte à l'intégrité des membres honnêtes du même secteur.

Sans une mise en application efficace, le Ministère de la Consommation et du Commerce est d'avis que le public et les organisations considéreront éventuellement une loi sur la protection des renseignements personnels comme une loi mal faite.

**Quelles seraient les mesures de mise en application autorisées en vertu de la loi proposée?**

La loi proposée offrirait diverses options pour sa mise en application. Elle permettrait notamment :

- de soumettre les litiges à la médiation ou de recommander une médiation extérieure;
- d'ordonner aux organisations de modifier leurs pratiques d'information de manière à se conformer aux dispositions de la loi (par ex., des ordonnances exécutoires);
- de publiciser les conclusions d'enquêtes;
- de publiciser les infractions pour lesquelles une accusation pourrait être portée et une action intentée.

Comme pour d'autres domaines de réglementation, il ne serait pas nécessaire de recourir à tous les pouvoirs conférés par la loi proposée pour résoudre la plupart des plaintes et des différends. En fait, si l'on en juge d'après l'expérience du Commissariat à la protection de la vie privée du Québec, on s'attend à ce que la médiation et la consultation viennent à bout de résoudre la plupart des plaintes et des différends.

En vertu de la loi proposée, si une personne croit qu'une organisation n'a pas recueilli, utilisé ou divulgué ses données personnelles conformément aux dispositions de la loi, la personne devrait d'abord communiquer directement avec l'organisation pour essayer de régler le problème. Si les parties ne parviennent pas à dénouer la situation, la médiation peut ensuite être autorisée.

La loi proposée établirait des mesures à prendre pour les plaintes individuelles ou d'autres motifs raisonnables comme : l'information d'un employé préoccupé ou un compétiteur qui voit un avantage injuste acquis en raison d'une violation de la loi sur la protection des renseignements personnels.

Un peu dans la même veine que la législation fédérale, la loi proposée prévoirait la « protection du dénonciateur » afin de protéger de représailles les employés qui mettent à jour des infractions à la loi sur la protection des renseignements personnels.

La loi proposée accorderait des pouvoirs d'enquête semblables à ceux prévus par d'autres lois régissant les activités commerciales et la protection du consommateur. Ces pouvoirs s'étendraient aux enquêtes visant à obtenir des renseignements dans les cas où il y aurait des motifs raisonnables et probables de croire à une infraction. Des mandats de perquisition seraient nécessaires pour

recueillir une preuve relative à une infraction possible ou entrer dans une résidence personnelle en vue de chercher une preuve d'infraction possible.

En vertu de la loi proposée, il serait défendu de faire obstruction à une enquête ou de détruire une preuve.

**Ordonnances exécutoires et promesses**

En vertu de la loi proposée, des ordonnances exécutoires permettraient d'assurer que les organisations prennent des recours sans porter de sanctions ou de blâmes. Pour rendre une ordonnance, il faudrait qu'il y ait des motifs raisonnables et probables de croire qu'une infraction a été commise. Par exemple, si des renseignements étaient utilisés de manière inacceptable ou si on avait refusé à une personne l'accès à ses données personnelles, une ordonnance pourrait exiger d'une organisation qu'elle se plie à au moins une des dispositions suivantes :

- fournir à la personne ses données personnelles;
- cesser ou modifier une pratique d'information particulière prohibée (comme cesser de divulguer des données personnelles à un tiers);
- mettre en œuvre des procédures visant à assurer la conformité à la loi proposée (comme des mesures en matière de documentation ou de sécurité).

Dans certains cas, une organisation pourrait aussi faire une promesse de conformité volontaire. Une promesse obligatoire en droit signifie qu'un recours volontaire sera pris avant que ne soit rendue une ordonnance de conformité. Cette promesse aurait la même force de loi qu'une ordonnance et serait aussi publique. La violation d'une ordonnance de conformité ou d'une promesse constituerait une infraction.

En vertu de la loi proposée, la proposition d'une promesse ne garantirait pas son acceptation et ne signifierait pas non plus qu'un organisme d'exécution ne rendrait pas une ordonnance de conformité ou ne veillerait pas l'application de mesures plus rigoureuses.

En proposant ou en faisant une promesse, une organisation n'admettrait pas une faute quelconque. Cependant, la promesse pourrait engager une organisation à prendre une mesure qu'elle n'aurait pas prise autrement (comme de publier des avis spéciaux à l'intention des clients ou du public, pour information).

**Appels**

La possibilité d'interjeter appel d'une décision est un principe fondamental de nombreux régimes de réglementation. Une personne ou une organisation qui est assujettie à des décisions administratives ayant des conséquences matérielles comme une ordonnance de conformité, a souvent le droit d'en appeler de ces décisions.

En vertu de la loi sur la protection des renseignements personnels, proposée par l'Ontario, un processus d'appel pourrait être créé. L'appel pourrait être entendu par un organisme indépendant comme une cour ou un tribunal spécialisé qui est indépendant du preneur de décision dont le

jugement est porté en appel. De tels appels sont prévus dans plusieurs lois régissant les normes du marché (comme la *Loi sur les pratiques de commerce).*

Un tribunal spécialisé peut souvent offrir une meilleure compréhension des questions et disposer des appels de manière plus opportune et économique que les cours. Une méthode rapide de résolution de litiges peut bien servir les organisations et les personnes.

Si un tribunal était créé, il serait toujours possible de saisir une cour d'un appel pour des questions de droit.

**<u>Question 12</u> : La loi sur la protection des renseignements personnels, proposée par l'Ontario, devrait-elle prévoir une possibilité d'appel sans qu'il soit nécessaire de se présenter devant la cour?**

Oui, un processus administratif devrait être prévu pour interjeter appel en cas de poursuite.

Non, le seul mécanisme d'appel devrait être les tribunaux.

**Qu'est-ce qui constituerait une infraction en vertu de la loi proposée?**

La plupart des problèmes d'application de la loi seraient vraisemblablement résolus par la médiation, les ordonnances de conformité et les promesses. Les poursuites relativement à une infraction ne seraient intentées que dans le cas d'une transgression délibérée de la loi proposée.

Les infractions possibles en vertu de la loi pourraient comprendre entre autres une transgression des principales dispositions de la loi :

- recueillir, utiliser ou divulguer des données personnelles contrairement aux dispositions de la loi proposée;
- refuser de donner, à des particuliers, accès à leurs données personnelles;
- obtenir par fraude les données personnelles de quelqu'un d'autre;
- faire obstruction à des enquêtes en détruisant ou en aliénant des données personnelles ou encore en mentant aux enquêteurs, par exemple;
- violer une ordonnance de conformité ou une promesse de conformité volontaire.

Les amendes autorisées en vertu de la loi proposée sont compatibles avec celles prévues dans d'autres lois. La plupart des lois administratives imposent actuellement des amendes pouvant s'élever jusqu'à 50 000 dollars pour les personnes et jusqu'à 500 000 dollars pour les sociétés ou autres types d'organisation.

**Une personne doit-elle simplement se fier à la mise en application de la loi proposée?**

En vertu de la loi sur la protection des renseignements personnels, proposée par l'Ontario, les particuliers pourraient intenter des poursuites devant une cour civile, pour des dommages découlant d'une violation de leurs droits dans le cadre de la loi proposée.

Afin de maintenir leur capacité de faire appliquer la loi proposée avec efficacité et de résoudre les litiges sur la protection des renseignements personnels, les personnes chargées de cette mise en application de la loi proposée ne pourraient pas être citées comme témoins dans des poursuites au civil.

*La possibilité de chercher un recours par le biais d'intérêts privés représente une particularité de la common law. La loi sur les normes du marché n'occulte pas le plus souvent les droits d'une instance civile.*

**Question 13 : Êtes-vous d'accord pour que la loi proposée fournisse ce qui suit :**

| | |
|---|---|
| Médiation : | Oui___ Non ____ |
| Pouvoir d'enquête : | Oui___ Non ____ |
| Ordonnance de conformité : | Oui___ Non ____ |
| Promesses de conformité volontaire : | Oui___ Non ____ |
| Appui aux recours civils : | Oui___ Non ____ |
| Infractions : | Oui___ Non ____ |

Si vous croyez qu'il devrait y avoir d'autres pouvoirs d'enquête ou d'exécution de la loi, veuillez les suggérer.

## Conclusion

**La présente proposition ne représente pas le point de vue final de l'Ontario sur la meilleure façon de structurer une loi ontarienne sur la protection des renseignements personnels.**

**Vos commentaires et vos points de vue sont essentiels dans le choix de la forme que prendra la loi sur la protection des renseignements personnels en Ontario. Nous apprécierons tous vos commentaires sur les questions précises que nous vous avons posées ainsi que sur tout autre aspect de la loi proposée. Veuillez indiquer si vous faites vos commentaires à titre individuel ou en tant que représentant d'une organisation.**

**Veuillez envoyer vos commentaires à n'importe laquelle des adresses suivantes :**

Ministère de la Consommation et du Commerce
Consultation sur la protection des renseignements personnels
250, rue Yonge, 35e étage
Toronto (Ontario)
M5B 2N5

**Télécopieur : (416) 326-8885**

**privacy@ccr.gov.on.ca**

**Le ministère de la Consommation et du Commerce a reçu pour directive de consulter le public sur la meilleure façon de charpenter une loi ontarienne sur la protection des renseignements personnels. Toutes les données personnelles que vous fournissez sont protégées en vertu de la *Loi sur l'accès à l'information et la protection des renseignements personnels*. Ces données personnelles nous aiderons à entreprendre cette consultation et à en évaluer les résultats; cela pourrait entraîner la divulgation de vos commentaires à d'autres participants, institutions et autres parties intéressées pendant et après la consultation. Votre identité ne sera en aucun cas dévoilée sans votre consentement.**

**Si vous désirez poser des questions sur la cueillette, l'utilisation ou la divulgation de ces données personnelles, vous pouvez entrer en contact avec :**

**Le coordinateur de l'accès à l'information et de la protection de la vie privée**
**Ministère de la Consommation et du Commerce**
**(416) 326-8470**

## ANNEXE A : Code type CSA sur la protection des renseignements personnels

Le document qui suit, tiré de la norme CAN/CSA-Q830-96 intitulée *Code type sur la protection des renseignements personnels,* a été reproduit avec la permission de CSA International. Il est protégé par le droit d'auteur de CSA International dont les bureaux sont situés au 178, boulevard Rexdale, Etobicoke, en Ontario, M9W 1R3. Bien que la reproduction de ce matériel ait été autorisée, CSA International ne sera pas tenu responsable de la façon dont l'information est présentée, ni de son interprétation.

Pour obtenir de plus amples renseignements sur ce code type de CSA International ou pour acheter un exemplaire de la norme, veuillez communiquer avec cet organisme en téléphonant au (416) 747-4044 ou au 1 (800) 463-6727, ou visiter son site Web à http://www.cswa-international.org

Dix principes interdépendants constituent la base du *Code type sur la protection des renseignements personnels.* Chaque principe doit être lu conjointement avec le commentaire qui l'accompagne.

**1. Responsabilité**

Une organisation est responsable des données personnelles qu'elle contrôle et elle doit désigner une personne ou des personnes chargées d'assurer la conformité aux principes décrits ci-après.

**2. Identification des buts**

L'organisme doit indiquer à quelles fins sont destinées les données personnelles qu'il recueille, au moment de la cueillette de ces données ou avant celle-ci.

**3. Consentement**

La connaissance et le consentement de la personne concernée sont deux éléments requis pour procéder à la cueillette, à l'utilisation ou à la divulgation de données personnelles, sauf lorsque cela est inapproprié.

**4. Limitation de la cueillette**

Seules les données personnelles qui sont nécessaires aux fins désignées par l'organisation seront recueillies. L'information sera recueillie par des moyens licites et équitables.

**5. Limitation de l'utilisation, de la divulgation et de la conservation des données personnelles**

Les données personnelles seront utilisées ou communiquées aux seules fins pour lesquelles elles auront été recueillies, sauf consentement de la personne concernée ou comme l'exige la loi. Elles seront conservées aussi longtemps que nécessaire, jusqu'à ce qu'elles répondent aux fins auxquelles elles sont destinées.

**6. Exactitude**

Les données personnelles seront exactes, complètes et à jour de façon à répondre aux fins auxquelles elles sont destinées.

**7. Mesures de protection**

Les données personnelles feront l'objet de mesures de protection appropriées à leur niveau de sensibilité.

**8. Transparence**

L'organisation rendra facilement accessible l'information sur sa politique et ses pratiques en matière de gestion de données personnelles.

**9. Accès à l'information**

Toute personne qui en fait la demande sera informée de l'existence, de l'utilisation et de la divulgation de données personnelles la concernant et pourra accéder à celles-ci. Elle pourra contester l'exactitude et l'intégralité de ces données et les faire modifier, le cas échéant.

**10. Mise en question de la conformité**

Une personne pourra contester la conformité de l'organisation aux principes susmentionnés, auprès de ceux ou celles qui en sont responsables.

## ANNEXE B : Secteur de la santé – Règles en matière de protection des données personnelles de santé

Les renseignements exacts et opportuns jouent un rôle capital dans la prise de décisions relative au système de santé – qu'il s'agisse de faire un diagnostic pour des soins urgents, de planifier l'organisation et la prestation de services de santé ou d'explorer de nouvelles façons améliorées de traiter des maladies.

Les données médicales étant très personnelles, il importe de protéger la vie privée des gens. C'est pourquoi il est nécessaire d'établir des limites qui déterminent de quelle façon et à quel moment des données médicales peuvent être communiquées.

Les règles imposées par la loi et qui s'appliquent aux données médicales, dans le secteur de la santé, doivent refléter un juste équilibre entre la protection des renseignements personnels et l'assurance qu'elles peuvent être utilisées avec soin et à bon escient pour améliorer le maintien et la gestion du système de santé.

Il est aussi important que les mêmes règles s'appliquent à toutes les parties du secteur de la santé, depuis les cabinets de médecins, jusqu'aux laboratoires et salles d'urgence. Des règles claires pour les données médicales personnelles renforceront les réformes gouvernementales, telles que la réforme des soins primaires et l'initiative « Systèmes intelligents pour la santé » et autre initiative visant à créer des services de santé intégrés. Sans règles communes, ces initiatives destinées à créer une meilleure coordination des services de santé et à planifier des améliorations au système de santé sur des bases solides pourraient être gravement compromises.

Le ministère de la Santé et des Soins de longue durée a mis la dernière main aux règles prévues par la loi visant à protéger les données médicales personnelles.

Le Ministère a mené deux séries de consultations poussées. En juin 1996, un document de consultation intitulé *Cadre législatif pour l'information sur la santé* a été diffusé à grande échelle aux fins de commentaires, et des tables rondes régionales ont été dirigées par l'adjoint parlementaire du ministre Helen Johns. En novembre 1997, un projet de loi intitulé *Loi sur la protection des renseignements médicaux personnels* a été élaboré aux fins de discussion et largement distribué aux fins de commentaires. Par la suite, des tables rondes régionales ont été animées par l'adjoint parlementaire du ministre Tim Hudak. Ces dernières consultations avaient pour but de mettre au courant les parties intéressées de l'évolution des mesures législatives depuis les dernières consultations et de les inviter à soumettre des observations.

Une fois que la loi ontarienne sur la protection des renseignements personnels sera mise en place, les règles touchant les données médicales, dans le secteur de santé, seront probablement incorporées dans le texte législatif à titre de code dans une annexe distincte. Le ministère de la Santé et des Soins de longue durée tiendra des consultations sur les règles proposées dans un proche avenir.

Pour obtenir un exemplaire du document de consultation publié, veuillez communiquer avec ce ministère au (416) 327-4327, ATS 1 800-387-5559 ou au 1 800-268-1153.

**ISBN 0-7778-9993-0**

**07/2000**

**© Imprimeur de la Reine pour l'Ontario, 2000**